International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

A Robust Audio Watermarking Method Using Advanced Encryption Technique.

Nazia Anjum & G. Deepika
M.Tech (DECE) RRS College of Engineering and Technology
Associate Professor RRS College of Engineering and Technology
naziaanjum.20@gmail.com & deepikareddygade@gmail.com

Abstract.

This paper exhibits a novel high-limit sound watermarking framework to install information and concentrate them in somewhat correct way by changing a portion of the extents of the FFT range. The key thought is to partition the FFT range into short casings and change the extent of the chose FFT tests utilizing Fibonacci numbers. Late rise in advanced innovation on broadband correspondence and mixed media information conveyance in computerized arrange opened many difficulties and open doors for analysts. Easy to-utilize programming and diminishing costs of computerized gadgets have made it workable for customers from all around the globe to make and trade interactive media information. Broadband Internet associations and blunder free transmission of information encourage individuals to convey vast sight and sound documents and make indistinguishable advanced duplicates of them. Advanced watermarking is characterized as system which specifically inserts and concentrates the information with security key from the host motion by proposed DWT to compute singular encryption and unscrambling. The primary test in computerized sound watermarking is that if the perceptual straightforwardness parameter is settled, the plan of a watermark framework can't acquire high strength and a high watermark information rate in the meantime. The consequences of this examination are the improvement and execution of sound watermarking calculations with powerful outcomes.

Keywords: Information security, Copyright protection, Audio, Audio Watermark, Key frame, DWT.

1. Introduction

With the increasing reliance on digital media and the rapid growth of Internet distribution possibilities, mechanisms of digital content distribution are continually becoming important and the intellectual property rights violation has become a serious concern for many institutions and organizations. In addition to difficulties in management of many illegal activities such as counterfeit, un-authentication, using/copying works without permission, etc. [1,2], another problem, which is related to a numerous of digital files including text, image, audio, and video is daily publishing without information of source, origin, authorship, copyright and intellectual property policy. To solve these problems, scientists have launched a variety of methods, mechanisms, as well as management policies to protect ownership, copyright content, and enhance security and safe-transmission of important information, avoid attacks and suspicion from the malicious third parties. Among all techniques suggested, digital watermarking is considered to be useful and meet most needs of data protection, authentication, and copyright products [3].

2. Literature Survey

Audio Watermarking is mainly classified in Spatial & Frequency Domain. In many literatures it has been

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

proved that frequency domain techniques give more advantage to the robustness of the watermark. In so many literatures like [4–10] authors discusses about embedding watermark in every frame of the audio. These techniques were working fine for various image processing attacks but were greatly suffering with collusion, frame averaging attacks. Also time complexity of such algorithm is very high due to embedding of a watermark in every frame. Afterwards, many researchers in [11–20] have used audio watermarking techniques based on scene changes. Idea was embedding the different part of the watermark in different scene. Scheme was robust to sustain many audio attacks like frame dropping, frame averaging etc. but limitation was first, taking time to identify scenes from audio. Secondly, scene change algorithm is highly content dependent so may not identify the exact scenes. Finally, the schemes get futile when there are no scene changes in the input audio and time complexity was quite higher for embedding and extraction of a watermark. Solution to this scheme was presented in the [21–30] which were key-frame based watermarking scheme. Here, key-frame was identified first and watermark was only embedded in key-frames. The scheme is pioneer and works well for many audio attacks like frame averaging, frame dropping, collusion etc. The scheme is solely depends on the identifying the key frames from the audio. Limitation of the scheme is that, there is a need of separate algorithm for key-frame detection and also if in frame dropping all the key frames are dropped then it is difficult to recover the watermark. Also, almost all the key-frames detection algorithms are content dependent so may not be most accurate to identify the same sequence of key-frames while watermark extraction process. From the above literature review, it is found that:

a. audio watermarking is different than image watermarking

b. It is essential to embed the watermark in more than one frame due to attacks like frame dropping and many other attacks.

c. Embedding watermark in all frames is always recommended but it discourages the performance of the scheme.

d. For embedding a watermark in selected frames, need of key-frame selection algorithm is essential, which add another complexity for research community. And get failed when there are no major scene changes in the audio.

e. There is no scheme which will just extract the watermark from frame, compare it with original watermark and declares that watermark is found in particular frame, thus stopping to extract frame from other frames, which saves amount of huge time.

So by observing all these issues, in this paper author propose a novel scheme for watermark embedding and extraction.

3. Audio Watermarking Scheme

This section gives details of watermark embedding & extraction algorithms. Also some of the assumptions are given below:

i. Audio input will be in .wav format.

ii. Watermark should be a binary image.

i. Watermark embedding

Figure 1 shows the block diagram of the proposed scheme. Initially, audio is taken as an input then it is decomposed into audio frames. Fibonacci series is generated which is used for the frame to embed the watermark. After embedding watermark, watermarked frames & un-watermarked frames are collected to form a watermarked video audio.

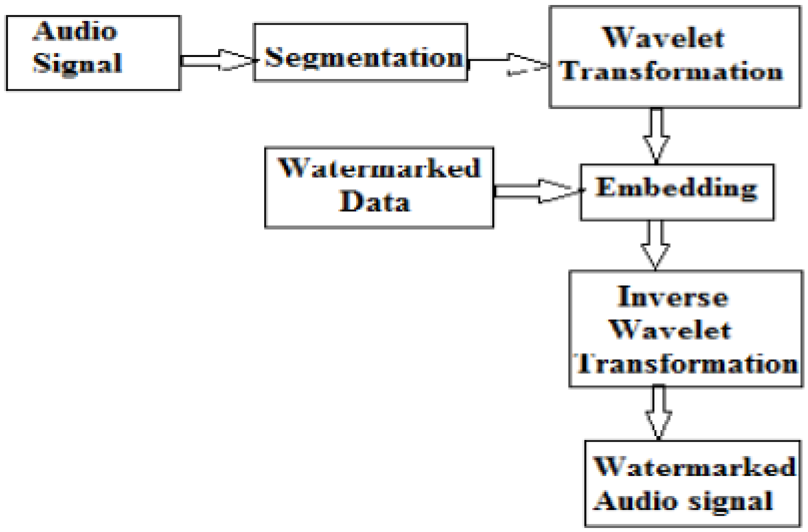

Fig-1 Audio watermarking scheme

Audio watermarking

Audio watermarking is a notable system of concealing information through sound signs. It is otherwise called sound steganography and has gotten a wide thought over the most recent couple of years. Up until now, a few systems for sound watermarking have been examined in writing by considering diverse applications and advancement positions. Perceptual properties of human sound-related framework (HAS) help to conceal various successions of sound through an exchanged flag. In any case, all watermarking methods face to an issue: a high power does not accompany high watermark information rate when the perceptual straightforwardness parameter is considered as settled. Besides, determination of a reasonable area, cover, and considering the issues related with information shrouded systems must be considered for outlining the way to accomplish an information concealed reason.

Embedding secret bits in Audio

In the previous couple of years, a few calculations for the implanting and extraction of messages in sound groupings have been proposed. The greater part of the created calculations abuse the attributes of the human sound-related framework (HAS) with a specific end goal to conceal information into the host motion in a perceptually straightforward way. Be that as it may, implanting mystery messages in advanced sound is typically a more troublesome process than installing messages in other media, for example, computerized pictures. What's more, the measure of information that can be implanted straightforwardly into a sound grouping is extensively lower than the measure of information that can be installed in pictures or video arrangements as a sound flag has a measurement under two-dimensional picture or video records. Then again, many assaults that are pernicious against picture steganography calculations (e.g. geometrical twists, spatial scaling, and so on.) are not pertinent to sound steganography plans . Implanting data into sound appears to be more secure because of less steganalysis procedures for assaulting to sound. Moreover, Natural affectability and trouble of taking a shot at sound brought about far less calculations and procedures when contrasted with pictures. Existing Audio Steganography plans can install messages in WAV, AU, AIFF and even MP3 sound document groups. Data covering up in sound signs has extensive variety of uses. The most imperative and evident use of Audio Steganography is clandestine correspondence utilizing harmless cover signals, similar to a phone discussion . Another application, known as (advanced) watermarking, alludes to installing an unpretentious stamp into a question, which can be utilized to distinguish the protest or go about as a copyright security of computerized media. For instance, an advanced watermark can be embedded into a bit of music so it can be checked naturally for installment purposes. One of the applications gives a system to installing vital control, illustrative or reference data in a given flag. This data can be utilized for following the utilization of a specific clasp, including charging for plugs and sound communicate. It can be utilized to track sound creation, control and adjustment history inside a given flag without the overhead connected with making a different header or history record. It can likewise be utilized to track access to a given flag. This data is critical in rights administration applications.

The human sound-related framework (HAS) works over a wide powerful range. When utilizing computerized pictures as cover records the trouble of the human eye to recognize hues is exploited, comparably, when utilizing advanced sound one can depend on the diverse affectability of the human ear with regards to hints of low and high power;

Normally, higher sounds are seen superior to bring down ones and it is in this way simpler to shroud information among low sounds without the human ear seeing the adjustment. What's more, there are some ecological twists so normal as to be disregarded by the audience in the majority of the cases. Such are the shortcomings of HAS that can be abused for expansion of information in sound signs. The impacts of human sound-related framework (HAS) in respect to Steganography are transient concealing and recurrence veiling. In transient concealing, a weaker capable of being heard flag on either side (pre and post) of a solid masker winds up noticeably subtle. Also, in recurrence veiling, if two signs happening all the while are near one another in recurrence, the more grounded covering sign may make the weaker flag indistinct.

There are two basic parameters to most computerized sound portrayals: test quantization strategy and fleeting examining rate. The most well known arrangement for speaking to tests of amazing advanced sound is a 16-bit straight quantization e.g.; Windows Audio-Visual (WAV) and Audio Interchange File Format (AIFF). Well known transient inspecting rates for sound incorporate 8 kHz (kilohertz), 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz and 44.1 kHz. Inspecting rate impacts information stowing away in that it puts an upper bound on the usable segment of the recurrence run. For the most part, the higher the examining rate is, the higher the usable information space. There are three issues which should be considered while managing sound documents :

- Audio documents in the Microsoft .wav (spot wave) organize, the range is mapped to (- 1, 1). For handling these signs, each esteem must be changed over to whole number arrangement.

- Human sound-related framework (HAS) is more delicate than Human visual framework (HVS). Varieties in the sound flag will be effortlessly seen.

- It is harder to control sound signs than the computerized pictures.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Matlab bolsters two sound document groups: WAV and AU sound records.

WAV records: WAV (or WAVE) is otherwise called Audio for Windows. It is a Microsoft and IBM sound document design standard for putting away a sound piece stream on PCs. It is the fundamental arrangement utilized on Windows frameworks for crude and ordinarily uncompressed sound. The standard piece stream encoding is the Pulse Code Modulation (PCM) design. It underpins multi-channel information, with up to 32 bits for every specimen. Au documents: The Au record design is a basic sound record arrange presented by Sun Microsystems. Perusing an .au document returns plentifulness esteems in the range [-1, +1]. It bolsters multichannel information in the accompanying configurations:

- 8-bit mu-law
- 8-, 16-, and 32-bit direct
- Floating-point

Here, WAV sound records are utilized for following reasons :

- It is the primary organization utilized on Windows frameworks for crude and commonly uncompressed sound.
- It could digitize sounds 100% devoted to the first source, in this way keeping up greatest sound quality.
- The wav document is anything but difficult to alter and control.

ii. Watermark extraction

Watermark Extraction is almost same process of the Watermark Embedding. In this paper a new way of watermark extraction is suggested which proved to be the best way to go for Ownership Proof

Figure 4, shows the block diagram of Watermark Extraction, which is almost similar as Watermark Embedding. Only difference is that instead of embedding watermark algorithm, watermark extraction algorithm is used. Also, watermark is finally displayed as per the similarity based on normalized correlation. Many researchers in their papers have recovered all the watermarks and their average is taken to form a recovered watermark. Limitation of these types of schemes are first, not an efficient in time and also some recovered watermarks which are recovered in good condition get disturbed due to the averaging operation. In this paper author has first extract the watermark from first frame, compare it with original if the difference is below threshold then watermark is displayed directly and algorithm terminates as the watermark is found in the first frame itself then there is no need to search it in the subsequent frame. Due to this change the extraction algorithm becomes most effi- cient in time & accurate. Also it becomes robust for other attacks if performed on some frames instead of all the frames.

4. Experimental Results

This part of the section highlights on the experimental results obtained during the implementation of this scheme.

Encryption

To scramble the watermark motion in to the host sound flag exhibit plot utilizes the added substance watermarking strategy. The host sound flag is partitioned into the portions of size N= 256, 512, 1024… and so on.

$X_k(i) = X(k \cdot N + i)$ i=0,1,2… ..N-1, K=0,1,2… ..

N=256, 1024

Where X(i) speak to the first host sound flag and Xk(i) speak to the kth fragment of the host sound. At that point each Xk(i) is deteriorated to Lth level wavelet change. The plan is executed utilizing Discrete Wavelet Transform (DWT) and Lifting Wavelet change (LWT). To implant the watermark into low recurrence part of the most noteworthy vitality of sound flag by exploiting recurrence cover impact of HAS the third level detail some portion of coefficients is chosen. In the wake of choosing the watermark inserting recipe the third surmised coefficients are changed as

Ak3 (i) =A k3 (i)+ α(k)w(k)r(i)

Where Ak3 (i) are third level rough coefficients. Where r(i) is the permuted pseudorandom double flag with zero mean which is the mystery key of the proprietor, α(k) and w(k) are the scaling parameter and watermark bit to be installed in kth section individually. The SNR between the first flag and the watermarked flag can be figured to quantify the intangibility of the watermarked flag.

In this technique we figure the scaling parameter α(k) for each section of host sound flag and after that insert as indicated by the guidelines for bit one or bit 0 of watermark flag. This variety of α(k) for each fragment considers the component of the host sound in that portion and after that figure the estimation of α(k), which is like finding the scaling parameter thinking about the perceptual straightforwardness of the host sound.

Decryption

The watermark decryption for the proposed scheme is to detect the watermark from the embedded signal the 3rd level DWT of the watermarked signal is computed. Then the coefficients $D_k^3{}'(i)$ are modified by the same pseudorandom signal r(i) used while embedding the watermark.

$$s(i) = D_k^3{}'(i)r(i)$$

Where $D_k^3{}'(i) = D_k^3 + \alpha(k)w(k)r(i)$ and s(i) wavelet coefficients modified by r(i).

$$\text{Therefore, } s(i) = D_k^3 + \alpha(k)w(k)r(i)r(i)$$

$$\sum s(i) = \sum D_k^3 r(i) + \sum \alpha(k)w(k)r2(i)$$

The expected value of the first term is approximately equal to zero and the value of $\sum r^2(i)$ is N (α(k) w(k) are independent of summation variation i) therefore the value of the equation is approximately equal to Nα(k)w(k), where N is the size of the segment. If the value of $\sum s(i)$ is greater than threshold the watermark bit one will be recovered and if the value of summation is less than the threshold the watermark bit 0 will be recovered.

Capacity

Knowing how much data can dependably be covered up in the flag is vital to clients, particularly when the plan gives them the capacity to change this sum. Knowing the watermarking access unit (or granularity) is likewise imperative; in reality, spreading the check over a full stable track forestalls sound gushing, for example. (A "watermark get to unit" is the littlest piece of a cover motion in which a watermark can be dependably recognized and the payload removed.)

Speed

A few applications require continuous implanting or potentially ongoing discovery. At last for such application the executed plan ought to have the capacity to implant and distinguish the installed watermark with fast.

Performance Tests:

In this area we give the consequences of strength trial of the three methods that we have made against a few types of assault. Unsettling influences considered in assessing watermarking frameworks are acknowledged utilizing the instrument "Stirmark Audio" and the encoder wav "lame.exe" to do the pressure/decompression MP3 with three distinct rates 128kbps, 64kbps.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

5. Conclusion

In this paper, we proposed a strong watermarking sound procedure working in the recurrence space. Fundamental objective of this theory is to build up the wise encoder and decoder model of hearty and secure sound watermarking. In the key advanced sound watermarking calculations and strategies are displayed. The alluded calculations are arranged by area utilized for embeddings a watermark and factual strategy utilized for encode and decipher of watermark bits. To expand the high piece rate we install the information in LSB of host sound in wavelet area. The wavelet area was decided for information covering up because of its low handling clamor and appropriateness for recurrence examination, as a result of its multiresolutional properties that give get to both to the most huge parts and subtle elements of flag's range. The wavelet space calculation produces stegoobjects perceptually barely segregated from the first sound clasp notwithstanding when LSBs of coefficients are adjusted. The sound watermark is included into the host sound. In proposed conspire we endeavor to implant the sound watermark in have sound flag. We have attempted to install the sound information of 0.5 sec's. To implant one piece of data we change just a single example in the host sound portion since our fundamental objective of watermarking is to expand the power and identification execution we wanted to contrasted due its prevalence with redress mistakes enhancing the bit blunder rate.

References

[1] http://en.wikipedia.org/wiki/Copyright, 22/01/2013.
[2] S. Ryoichi and Y. Hiroshi, Consideration on Copyright and Illegal Copy Countermeasures under IT Revolution, Joho Shori Gakkai Kenkyu Hokoku, vol. 2001, pp. 37–42, (2001).
[3] S. Katzenbeisser, On the Integration of Cryptography and Watermarks (invited paper), in International Workshop on Digital Watermarking 2003, Springer Lecture Notes in Computer Science, vol. 2939, pp. 50–60, (2003).
[4] Alam, Md. Jahangir−2, Asikuzzaman, Md.−1, Lambert, Andrew J.−3, Pickering and Mark R.−4, A Blind Digital audio Watermarking Scheme with Enhanced Robustness to Geometric Distortion, Digital Image Computing Techniques and Applications (DICTA), 2012 International Conference on, year: vol. 1, no. 1, pp. 1–8, (2012).
[5] Hasnaoui, M.−1 and Mitrea, M.−2, Semi-fragile watermarking for video surveillance applications, Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European, pp. 1782–1786, year (2012).
[6] Roy, Sudipta−3, Singh, Kh. Manglem−2, Singh and Th. Rupachandra−1, Robust video watermarking scheme based on visual cryptography, Information and Communication Technologies (WICT), 2012 World Congress on, pp. 872–877, year (2012).
[7] Koga, T.−2, Kondo, K.−3 and Yamaguchi, Y.−1, A Watermarking Method for Embedding Short Information Split into Audio and Video Signals, Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on, pp. 130–133, year (2012).
[8] Vural, C.−2 and Yildirim, I.−1, Reversible video watermarking based on histogram modification of motion compansated prediction error, Signal Processing and Communications Applications Conference (SIU), 2012 20th, pp. 1–4, year (2012).
[9] El Allali, A.−1, Elabbadi, J.−2 and Iben Elahaj, E.−3, Video object watermarking using 3D-Walsh Hadamard transform and Arnold transform, Multimedia Computing and Systems (ICMCS), 2012 International Conference on, pp. 119–124, year (2012).
[10] Dwivedi, V. V.−2 and Kothari, A. M.−1, Transform Domain Video Watermarking: Design, Implementation and Performance Analysis, Communication Systems and Network Technologies

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

(CSNT), 2012 International Conference on, pp. 133–137, year (2012).
[11] Yan Liu and Jiying Zhao, A new video watermarking algorithm based on 1D DFT and Radon transform, Elsevier Journal of Signal Processing, pp. 628–639, (2010).
[12] Xue Junxiaoa, Li Qingbinc and Li Zhiyong, A novel digital video watermarking algorithm, Science Direct International Conference on Advances in Engineering, pp. 90–94, (2011).
[13] P. W. Chan and M. Lyu, A DWT-based digital video watermarking scheme with error correcting code, in Proc. 5th Int. Conf. Information and Communications Security (ICICS2003), vol. 2836. Huhehaote City, China, Oct. 10–13, pp. 202–213, (2003).
[14] A. Piva, F. Bartolini and M. Barni, Managing copyright in open networks, IEEE Trans. Internet Computing, vol. 6, no. 3, pp. 18–26, May–Jun. (2002).