Secure & Robust Higher LSB Audio Stenography with Cryptography for Secure Data Transmission

Preeti Singh[#1], Praveen Yadav[*2]

[#] *M.Tech Scholar*
RCET, Bhilai, India
[1]preeti.116singh@gmail.com
[2]ypn.praveen@gmail.com
[*] *Assistant Professor, Department of ECE*
RCET, Bhilai, India

Abstract—**In this paper, we present a novel high bit rate LSB audio watermarking method that reduces embedding distortion of the host audio along with symmetric key cryptography. Using the proposed two-step algorithm, watermark bits are embedded into higher LSB layers, resulting in increased robustness against noise addition. In addition, listening tests showed that perceptual quality of watermarked audio is higher in the case of the proposed method than in the standard LSB method. Conventionally, a perceptual limit of three bits per sample is imposed to the basic LSB audio steganography method. The proposed algorithm makes use of minimum error replacement method for LSB adjustment and modified error diffusion method for decreasing SNR value. Subjective listening test proved that high perceptual transparency is accomplished even if four LSBs of host audio signal are used for data hiding. Using the proposed two-step algorithm, hidden bits are embedded into the higher LSB layers, resulting in increased robustness against noise addition.**

Keywords—**Audio steganography , LSB coding, Data cryptography Flipping , SNR & Robustness.**

I. Introduction

Multimedia data hiding techniques have developed a strong basis of steganography area with a growing number of applications like digital rights management, covert communications, hiding executables for access control, annotation etc[1]. In all application scenarios given above, multimedia steganography techniques have to satisfy two basic requirements. The first requirement is perceptual transparency, i.e. cover object (object not containing any additional data) and stego object (object containing secret message) must be perceptually indiscernible. The second constraint is high data rate of the embedded data. All the stego applications, besides requiring a high bit rate of the embedded data, have need of algorithms that detect and decode hidden bits without access to the original multimedia sequence (blind detection algorithm)[2]. While the robustness against intentional attack is not required, a certain level of robustness of hidden data against common signal processing as noise addition or MPEG compression may be necessary. LSB coding is one of the earliest techniques studied in the information hiding and watermarking area of digital audio (as well as other media types). The main advantage of the LSB coding method is a very high watermark channel bit rate and a low computational complexity of the algorithm, while the main disadvantage is considerably low robustness against signal processing modifications[3]. The perceptual quality of watermarked audio is higher in the case of the proposed method than in the standard LSB method is implementing in the Electronic Copyright Management System[4].

II. Literature Review

Data hiding in the least significant bits (LSBs) of audio samples in the time domain is one of the simplest algorithms with very high data rate of additional information. The LSB watermark encoder [5] usually selects a subset of all available host audio samples chosen by a secret key. The substitution operation on the LSBs is performed on this subset, where the bits to be hidden substitute the original bit values. Extraction process simply retrieves the watermark by reading the value of these bits from the audio stego object. Therefore, the decoder needs all the samples of the stego audio that were used during the embedding process. The random selection of the samples used for embedding introduces low power additive white Gaussian noise (AWGN) [6]. It is well known from the psychoacoustics literature that the human auditory system (HAS) is highly sensitive to AWGN. That fact limits the number of LSBs that can be imperceptibly modified during watermark embedding. The main advantage of the LSB coding method is a very high watermark channel bit rate; use of only one LSB of the host audio sample gives capacity of 44.1 kbps (sampling rate 44 kHz, all samples used for data hiding) and a low computational complexity. The obvious disadvantage is considerably low robustness, due to fact that simple random changes of the LSBs destroy the coded watermark. As the number of used LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. Making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased. Therefore, there is a limit for the depth of the used

LSB layer in each sample of host audio that can be used for data hiding [7]. Subjective listening test showed that, in average, the maximum LSB depth that can be used for LSB based watermarking without causing noticeable perceptual distortion is the fourth LSB layer when 16 bits per sample audio sequences are used. The tests were performed with a large collection of audio samples and individuals with different background and musical experience. None of the tested audio sequences had perceptual artifacts when the fourth LSB has been used for data hiding although in certain music styles, the limit is even higher than the fourth LSB layer. Robustness of the watermark, embedded using the LSB coding method, increases with increase of the LSB depth used for data hiding. Therefore, improvement of watermark robustness obtained by increase of depth of the used LSB layer is limited by perceptual transparency bound, which is the fourth LSB layer for the standard LSB coding algorithm.

III. PROPOSED METHODOLOGY

Data Hiding

1. Select Audio Wave file
2. Select Key File
3. Select Secrete data
4. Encrypt Secrete data using Symmetric key cryptography.
5. Select audio Samples as per key file content.
6. Hide encrypted data in selected audio samples.
7. Save Audio Data.

Data Extraction

1. Select Audio File.
2. Select Key file
3. Extract data (Encrypted).
4. Decrypt Data.
5. Save Data.

A. Symmetric Cryptography

Because symmetric key cryptography uses the same key for both decryption and encryption, it is much faster than public key cryptography, is easier to implement, and generally requires less processing power. A disadvantage of symmetric key cryptography is that the 2 parties sending messages to each other must agree to use the same private key before they start transmitting secure information. This may be impossible depending on the circumstances – because the 2 parties who want to communicate with each other through a secure means may be on different sides of the world. And this means that they will need a secure way to tell each other what the private key will be – if there were a secure way to do this,then the cryptography would not have been necessary in the first place n order to create that secure channel.

The advantage of using public key cryptography is that the public key used for encryption does not need to remain secure (that is why it's called "public" – because it does not matter if other people know about it). What often happens is that people use public key cryptography to create a shared session key and then they communicate through symmetric key cryptography [8] using the shared session key. This way they can get the best of both worlds – the performance/speed of shared key cryptography along with the convenience of public key cryptography.

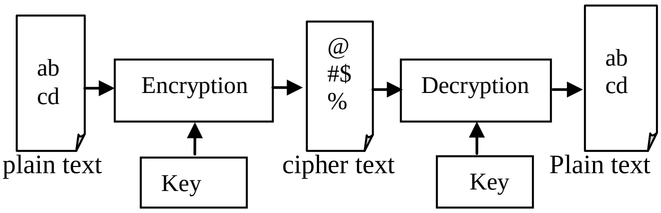

Figure 1. Symmetric Key Cryptography

The advantage of using public key cryptography is that the public key used for encryption does not need to remain secure (that is why it's called "public" – because it does not matter if other people know about it). What often happens is that people use public key cryptography to create a shared session key and then they communicate through symmetric key cryptography using the shared session key? This way they can get the best of both worlds – the performance/speed of shared key cryptography along with the convenience of public key cryptography.

B. Proposed LSB Method for Hiding

We developed a novel method that is able to shift the limit for transparent data hiding in audio from the fourth LSB layer to the sixth LSB layer, using a two-step approach. In the first step, a watermark bit is embedded into the I th LSB layer of the host audio using a novel LSB coding method. In the second step, the impulse noise caused by watermark embedding is shaped in order to change its white noise properties. The standard LSB coding method simply replaces the original host audio bit in the I th layer (i=1, 16) with the bit from the watermark bit stream. In the case when the original and watermark bit are different and I th LSB layer is used for embedding the error caused by watermarking is 2^i-1 quantization steps (QS) [9] (amplitude range is [-32768 to 32767]). The embedding error is positive if the original bit was 0 and watermark bit is 1 and vice versa. The key idea of the proposed LSB algorithm is watermark bit embedding that causes Minimal embedding distortion of the host audio. It is clear that, if only one of 16 bits in a sample is fixed and equal to the watermark bit, the other bits can be flipped in order to minimize the embedding error [10].

IV. DATA HIDING ALGORITHM

```
If host sample a>0
    If bit 0 is to be embedded
    If $a_{i-1}$ =0 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ = 11....1
    If $a_{i-1}$ =1 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ = 00....0
    If $a_{i+1}$ =0 then $\underline{a}_{i+1}$ =1
    Elseif $a_{i+2}$ =0 then $\underline{a}_{i+2}$ = 1
    ........
    Elseif $a_{15}$ =0 then $a_{15}$ =1
```

```
Else if bit 1 is to be embedded
If $a_{i-1}$ =1 then $\underline{a}_{i-1}\ \underline{a}_{i-2}$ ----- $\underline{a}_0$ =00....0
        If $a_{i-1}$ = 0 then $\underline{a}_{i-1}\ \underline{a}_{i-2}$ ----- $\underline{a}_0$ = 11.....1 and
        If $a_{i+1}$ = 1 then $\underline{a}_{i+1}$ =0
        Else if $a_{i+2}$ =1 then $\underline{a}_{i+2}$ = 0
        ........
        Else if $a_{15}$ =1 then $a_{15}$ =0
Else if bit 1 is to be embedded
If host sample a<0
        If bit 0 is to be embedded
         If $a_{i-1}$ =0 then $\underline{a}_{i-1}\ \underline{a}_{i-2}$ ----- $\underline{a}_0$ = 11....1
        If $a_{i-1}$ =1 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ = 00....0 and
            If $a_{i+1}$ =0 then $\underline{a}_{i+1}$ =1
            Else if $a_{i+2}$ =0 then $\underline{a}_{i+2}$ = 1
             ........
            Else if $a_{15}$ =0 then $a_{15}$ =1

        Else if bit 1 is to be embedded
         If $a_{i-1}$ =1 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ =00....0
        If $a_{i-1}$ =0 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ = 11.....1
        If $a_{i+1}$ =1 then $\underline{a}_{i+1}$ =0
        Elseif $a_{i+2}$ =0 then $\underline{a}_{i+2}$ = 1
        ........
        Elseif $a_{15}$ =1 then $a_{15}$ =0
        Else if bit 1 is to be embedded
```

For example, if the original sample value was 0...010002=810, and the watermark bit is zero is to be embedded into 4th LSB layer, instead of value 0...000002=010, that would the standard algorithm produce, the proposed algorithm produces sample that has value 0...001112=710, which is far more closer to the original one. However, the extraction algorithm remains the same; it simply retrieves the watermark bit by reading the bit value from the predefined LSB layer in the watermarked audio sample. In the embedding algorithm, the (i+1) th LSB layer (bit a_i) is first modified by insertion of the present message bit [11,12]. Then, the algorithm given below is run. In case that the bit a_i need not be modified at all due to being already at a correct value, no action is taken with that signal sample. Underlined bits (a_i) represent bits of watermarked audio.

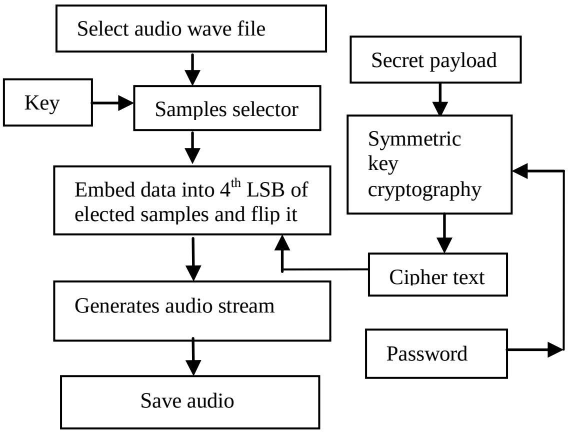

Figure 2. Data Hiding

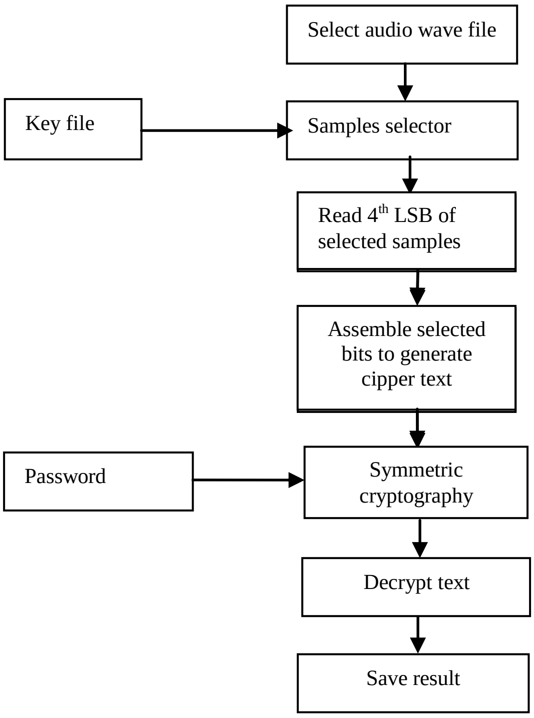

Figure 3. Data Extraction

V. Conclusion

We presented a reduced distortion bit-modification algorithm for LSB audio steganography along with symmetric key cryptography. The key idea of the algorithm is watermark bit embedding that causes minimal embedding distortion of the host audio. By listening tests it can be shown that described algorithm succeeds in increasing the depth of the embedding layer without affecting the perceptual transparency of the watermarked audio signal. The improvement in robustness in presence of additive noise is obvious, as the proposed algorithm obtains significantly lower bit error rates than the standard algorithm. The steganalysis of the proposed algorithm is more challenging as well, because there is a significant number of bits flipped in a number in bit layers and the adversary cannot identify exactly which bit layer is used for the data hiding.

References

[1] Anderson and Petitcolas 2001 Anderson, R; Petitcolas, F.: *On the limits of the steganography, IEEE Journal Selected Areas in Communications*, Volume 16(4), Page(s) 4,474-481.

[2] Bassia June 2001 Bassia; P., Pitas, I; Nikolaidis, N.: *Robust audio watermarking in the time domain*, IEEE Transactions on Multimedia, Volume 3, Issue 2, Page(s):232 – 241.

[3] Cedric 2000 Cedric, T.; Adi, R.,Mcloughlin, I.: *Data concealment in audio using a nonlinear frequency distribution of PRBS coded data and frequency-domain LSB insertion*, Proc. IEEE Region 10 International Conference on Electrical and Electronic Technology, Kuala Lumpur, Malaysia, pp 275-278

[4] Dumitrescu 2002 Dumitrescu, S.; Wu, W; Memon, N.: *On steganalysis of random LSB embedding in continuous-tone images*, Proc. International Conference on Image Processing, Rochester, NY,

pp 641-644.

[5] Fridrich 2002 Fridrich; J., Goljan; M., Du, R.:*Lossless Data Embedding New Paradigm in Digital Watermarking, Applied Signal Processing*, 2002, 2, pp 185-196

[6] Lee and Chen 2000 Lee; Y., Chen : *High capacity image steganographic model, IEEE Proceedings on Vision, Image and Signal Processing*, 147, 3, pp 288-294.

[7] Mintzerl ; Mintzer, F.; Goertzil, G.; Thompson, G.; *"Display of images with calibrated colour on a system featuring monitors with limited colour palettes*", Proceeding. SID International Symposium, pp 377-380;1988.

[8] [Mobasseri 1998] Mobasseri, B.: Direct *sequence watermarking of digital video using m-frames*, Proceeding International Conference on Image Processing, Chicago, IL, pp 399- 403.

[9] [Yeh and Kuo 1999] Yeh, C., Kuo, C.: *Digital Watermarking through Quasi m-Arrays, Proc. IEEE Workshop on Signal Processing Systems*, Taipei, Taiwan, 456-461. [Zwicker 1982] Zwicker, E.: Psychoacoustics, Springer Verlag, Berlin, Germany.

[10] Ahuja, B.; Kaur, M., *"High Capacity Filter Based Steganography",* International Journal of Recent Trends in Engineering, Vol. 1, No. 1, 2009

[11] Maitra, I. K.; Nag, S.; Datta, B.; Bandyopadhyay, S. K., "*Digital Steganalysis: Review on Recent Approaches"*, Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011

[12] Mohammed, A. F., "*Image Steganography by Mapping Pixels to Letters*", Journal of Computer Science 5 (1): pp. 33-38, 2009

[13] David, K., *"The History of Steganography", Proc. of First Int. Workshop on Information Hiding*, Cambridge,UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson (Ed.), pp.1-7

[14] Bender, W.; Gruhl, D.; Morimoto, N.; Lu, A., *"Techniques for data hiding"*, IBM Systems Journal, vol. 35, Issues 3&4, 1996, pp. 313-336.

[15] Kharrazi, M.; Sencar, H. T.; Memon, N., *"Image Steganography: Concepts and Practice*", WSPC, April 22, 2004

BIBLIOGRAPHY

Preeti Singh received her B.E. degree in Electronics & Telecommunication Engineering from M.P.Christian College of Engineering & Technology (affiliated to Pt. Ravishankar Shukla University), Raipur in 2008 and persuing her Mtech degree in Digital Electronics from Rungta College of Engineering & Technology(Affiliated to CSVTU), Bhilai. She is a lecturer in Electronics & Telecommunication department at G.D. Rungta college of engineering & Technology, Bhilai.

Professor Praveen Yadav B.E. from SSCET Bhilai, M.Tech(Digital electronics) from RCET Bhilai, assistant professor of Electronics & Telecommunication, RCET, Bhilai, India. His research interests signal processing and communication. He has 6 yrs of experience at the Post-graduate and under-graduate teaching in Chhattisgarh Swami Vivekanand University, Bhilai. He has already got several Academic Distinctions in Degree level/Recognition/Awards from various prestigious Institutes and Organizations. He has published 3 Res earch papers in International & Indian Journals.