ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.3

Data Hiding with Adaptive Bitstream Steganography Cryptosystem

R.Keerthana[1], K.Meena[2], B.Divya Bharathi[3], M.S.Vijaykumar[4]
BE Student[1, 2, 3], Assistant Professor[4]
Department of IT
Tejaa Shakthi Institute of Technology for Women, Coimbatore, India

Abstract:
More recently, people are hiding secret messages in graphics images or audio or video. The method of embedding the actual message on the other Medium such as image, sound files etc are called as "Stenography".To reduce the complexity for minimizing joint distortion, an coding method to decompose the joint distortion (abbreviated to DeJoin) into distortion on individual pixels and thus the message can be anciently embedded with syndrome trellis codes (STCs).In proposed system use very high secure to hide the data by using audio files. The algorithms used are LSB (LEAST SIGNIFICANT BIT)

1. INTRODUCTION

STEGANOGRAPHY is a technique for covert communication, which aims to hide secret messages into ordinary digital media without drawing suspicion [1]–[4]. Currently, most approaches on content adaptive steganography are based on the model of minimizing distortion between the cover and the corresponding stego object. Most adaptive steganographic methods adopted additive distortion fuchtions, such as HUGO, WOW, UNIWARD, HILL, and MiPOD in which the distortion is defined by assigning costs to individual cover elements. In additive distortion model, the modifications on pixels are assumed to be independent and thus minimizing the overall costs is equivalent to minimizing the sum of costs of individual changed elements. For additive distortion based methods, the practical message embedding is usually realized by the efficient coding method, syndrome trellis codes (STCs) [11], which can approach the lower bound of average embedding distortion for additive model.

2. DEFINING JOINT DISTORTION WITH

SMD Principle

In the above section, we propose a general method for embedding messages by minimizing joint distortion. The joint distortion can be defined in several manners, e.g., extending the Gaussian models used in [9] from single pixel to multi-pixels or generalizing the SMD based method [12], [13]. For fairly comparing with the methods in [12], [13], we give some examples on how to define joint distortion based on the principle of SMD.

3. RESISTING SELECTION CHANNEL AWARE DETECTION BY USING LARGER PIXEL BLOCKS

Recent advances in steganalysis show that, by using Selection-Channel-Aware (SCA) features, the Warden can reduce the error rates when detecting adaptive steganography. The maxSRMd2 model is a SCA version of SRM has the same dimension with SRM. When using the SCA features, the Warden needs to estimate the change probabilities of each pixel, which is easy for detecting additive schemes, such as HILL and MiPOD.

Drawback of Existing System

Suppose the receiver does not have embedding key, but posses the encryption keys only, the image can still be decrypted from the encrypted bit stream naturally with some distortion. It does not provide satisfactory security

Proposed System

The algorithm used is Least Significant Bit Algorithm. Information hiding techniques proposed to embed secret information within audio file using LSB.LSB method allows large amount of secret information to be encoded in an audio file.

Advantages of Proposed System

It provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. It also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

4. CONCLUSION

In this paper, we proposed a framework to improve the security of adaptive steganography by defining joint distortion functions on pixel blocks, which exploits the interactive impact of changes between adjacent pixels. The proposed system consists of the encryption applied to the audio files through the wave file format. The noise bits in the audio file are removed and the original message is hidden. In the future, the steganography can be implemented with help of video file.

5. REFERENCES

[1]. J. Fridrich, "Steganography in Digital Media: Principles, Algorithms and Applications," Cambridge University Press, 2009.

[2]. B. Li, J. He, J.w. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142-172, 2011.

[3] .Z. Xia, X. Wang, X. Sun, and B. Wang, "Steganalysis of least significant bit matching using multi-order differences," Security and Communication Networks, vol. 7, no. 8, pp. 1283-1291, 2014.

[4] .Z. Xia, X. Wang, X. Sun, Q. Liu, and N. Xiong, "Steganalysis of LSB matching using differences between nonadjacent pixels," Multimedia Tools and Applications, vol. 75, no. 4, pp. 1947-1962, 2016.

[5] .T. Pevny, T.Filler, and T. Bas, "Using high-dimensional image models to perform highly undetectable steganography," Proc. of International Workshop on Information Hiding, vol. LNCS 6387, pp. 161-177, 2010.

[6]. V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," Proc. of IEEE Workshop on Information Forensic and Security, pp. 234-239, 2012

[7]. J. Fridrich and J. Kodovsky, "Multivariate Gaussian model for designing additive distortion for steganography," Proc. of IEEE ICASSP, Vancou- ver, BC, May 26-31, 2013.

[8] .V. Sedighi, R. Cogranne, J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," IEEE Trans. on Inf. Forensics Security, vol. 11, no. 2, pp. 221-234, 2016.

[9]. T. Filler, J. Judas, and J.Fridrich, "Minimizing additive distortion in steganography using syndrome trellis codes," IEEE Trans. on Inf.Forensics Security, vol. 6, no. 1, pp. 920-935, 2011.

[10]. B. Li, M. Wang, X. L. Li, and S. Tan, "A strategy of clustering modification directions in spatial image steganography," IEEE Trans.on Inf. Forensics Security, vol. 10, no. 9, pp. 1905-1917, 2015.

[11]. T. Denemark and J. Fridrich, "Improving steganographic security by synchronizing the selection shannel," Proc. of 3rd Workshop on I-H&MMSec, Portland, Oregon, June 17-19, 2015.