Springer Link

A Secure High-Capacity Video Steganography Using Bit Plane Slicing Through (7, 4) Hamming Code

Advanced Computational and Communication Paradigms pp 85-98 | Cite as

- Ananya Banerjee (1) Email author (anaanya.2011@gmail.com)
- Biswapati Jana (1)

1. Department of Computer Science, Vidyasagar University, , Midnapore, India

Conference paper
First Online: 21 April 2018

Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 706)

Abstract

Achievement of high-capacity data hiding using a digital media is an important research issue in the field of steganography. In this paper, we have introduced a novel scheme of data hiding directly within the video stream **using** bit plane slicing through (7, 4) Hamming code with the help of shared secret key. In the proposed scheme, a secret logo image is embedded within the cover video stream for authentication and ownership identification through Hamming code based video steganography. Each frame of secret video has been separated into individual three basic color blocks (R, G and B) and then partitioned into (3 × 3) pixel blocks. After that, each color block is sliced up into 4 bit planes starting from LSB plane. The pixels' positions of cover images are randomly selected by Pseudorandom Number Generator (PRNG) using a shared secret seed value and data embedding performed using (7, 4) Hamming code. As a result, 36 bits secret data can be embedded within a (3 × 3) pixel block which is almost eight times greater than Ramadhan and Khaled's scheme (Systems, applications and technology conference (LISAT), 2014 IEEE Long Island, 2014) [1]. Here, we achieve a high payload with good visual quality stego video. **Furthermore, the video compression is lossless so the video file size is strictly preserved for post-data embedding**.

Keywords

Video steganography Hamming code Least significant bit (LSB) Bit plane Data hiding

References

1. Mstafa, R.J., Elleithy, K.M.: A highly secure video steganography using Hamming code (7, 4). In: Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island. IEEE (2014)
Google Scholar (https://scholar.google.com/scholar?q=Mstafa%2C%20R.J.%2C%20Elleithy%2C%20K.M.%3A%20A%20highly%20secure%20video%20steganography%20using%20Hamming%20code%20%287%2C%204%29.%20In%3A%20Systems%2C%20Applications%20and%20Technology%20Conference%20%28LISAT%29%2C%202014%20IEEE%20Long%20Island.%20IEEE%20%282014%29)

2. Cao, Z., Yin, Z., Hu, H., Gao, X., Wang, L.: High capacity data hiding scheme based on (7, 4) Hamming code. SpringerPlus **5**(1), 175 (2016)
CrossRef (https://doi.org/10.1186/s40064-016-1818-0)
Google Scholar (http://scholar.google.com/scholar_lookup?title=High%20capacity%20data%20hiding%20scheme%20based%20on%20%287%2C%204%29%20Hamming%20code&author=Z.%20Cao&author=Z.%20Yin&author=H.%20Hu&author=X.%20Gao&author=L.%20Wang&journal=SpringerPlus&volume=5&issue=1&pages=175&publication_year=2016)

3. Hu, S.D.: A novel video steganography based on non-uniform rectangular partition. In: 2011 IEEE 14th International Conference on Computational Science and Engineering (CSE). IEEE (2011)
Google Scholar (https://scholar.google.com/scholar?q=Hu%2C%20S.D.%3A%20A%20novel%20video%20steganography%20based%20on%20non-uniform%20rectangular%20partition.%20In%3A%202011%20IEEE%2014th%20International%20Conference%20on%20Computational%20Science%20and%20Engineering%20%28CSE%29.%20IEEE%20%282011%29)

4. Yadav, P., Mishra, N., Sharma, S.: A secure video steganography with encryption based on LSB technique. In: 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). IEEE (2013)
Google Scholar (https://scholar.google.com/scholar?q=Yadav%2C%20P.%2C%20Mishra%2C%20N.%2C%20Sharma%2C%20S.%3A%20A%20secure%20video%20steganography%20with%20encryption%20based%20on%20LSB%20technique.%20In%3A%202013%20IEEE%20International%20Conference%20on%20Computational%20Intelligence%20and%20Computing%20Research%20%28ICCIC%29.%20IEEE%20%282013%29)

5. Dasgupta, K., Mandal, J.K., Dutta, P.: Hash based least significant bit technique for video steganography (HLSB). Int. J. Secur. Priv. Trust Manage. (IJSPTM) **1**(2), 1–11 (2012)
Google Scholar (https://scholar.google.com/scholar?q=Dasgupta%2C%20K.%2C%20Mandal%2C%20J.K.%2C%20Dutta%2C%20P.%3A%20Hash%20based%20least%20significant%20bit%20technique%20for%20video%20steganography%20%28HLSB%29.%20Int.%20J.%20Secur.%20Priv.%20Trust%20Manage.%20%28IJSPTM%29%201%282%29%2C%201%E2%80%9311%20%282012%29)

6. Banik, B.G., Bandyopadhyay, S.K.: Image Steganography using BitPlane complexity segmentation and hessenberg QR method. In: Proceedings of the First International Conference on Intelligent Computing and Communication (pp. 623–633). Springer Singapore

Google Scholar (https://scholar.google.com/scholar?q=Banik%2C%20B.G.%2C%20Bandyopadhyay%2C%20S.K.%3A%20Image%20Steganography%20using%20BitPlane%20complexity%20segmentation%20and%20hessenberg%20QR%20method.%20In%3A%20Proceedings%20of%20the%20First%20International%20Conference%20on%20Intelligent%20Computing%20and%20Communication%20%28pp.%20623%E2%80%93633%29.%20Springer%20Singapore)

7. Fridrich, J., Du, R., Meng, L. Steganalysis of LSB encoding in color images. In: Proceedings of ICME 2000, Jul.–Aug. 2000, N.Y., USA
Google Scholar (https://scholar.google.com/scholar?q=Fridrich%2C%20J.%2C%20Du%2C%20R.%2C%20Meng%2C%20L.%20Steganalysis%20of%20LSB%20encoding%20in%20color%20images.%20In%3A%20Proceedings%20of%20ICME%202000%2C%20Jul.%E2%80%93Aug.%202000%2C%20N.Y.%2C%20USA)

8. Westfield, A., Pfitzmann, A.: Attacks on steganographic systems. In: Proceedings of 3rd Info. Hiding Workshop, Dresden, Germany, Sept. 28–Oct. 1, pp. 61–75 (1999)
Google Scholar (https://scholar.google.com/scholar?q=Westfield%2C%20A.%2C%20Pfitzmann%2C%20A.%3A%20Attacks%20on%20steganographic%20systems.%20In%3A%20Proceedings%20of%203rd%20Info.%20Hiding%20Workshop%2C%20Dresden%2C%20Germany%2C%20Sept.%2028%E2%80%93Oct.%201%2C%20pp.%2061%E2%80%9375%20%281999%29)

9. University of Mannheim, Department of Computer science. http://ls.wim.uni-mannheim.de/de/pi4/research/projects/retargeting/test-sequences/ (http://ls.wim.uni-mannheim.de/de/pi4/research/projects/retargeting/test-sequences/)

10. Xu, W., Wang, R.D., Shi, Y.Q.: Data hiding in encrypted H.264/AVC video streams by codeword substitution. IEEE Trans. Inform. Forens. Secur. **9**(4), 596–606 (2014)
CrossRef (https://doi.org/10.1109/TIFS.2014.2302899)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Data%20Hiding%20in%20Encrypted%20H.264%2FAVC%20Video%20Streams%20by%20Codeword%20Substitution&author=Dawen.%20Xu&author=Rangding.%20Wang&author=Yun%20Q..%20Shi&journal=IEEE%20Transactions%20on%20Information%20Forensics%20and%20Security&volume=9&issue=4&pages=596-606&publication_year=2014)

Copyright information

About this paper

Cite this paper as:

Banerjee A., Jana B. (2018) A Secure High-Capacity Video Steganography Using Bit Plane Slicing Through (7, 4) Hamming Code. In: Bhattacharyya S., Chaki N., Konar D., Chakraborty U., Singh C. (eds) Advanced Computational and Communication Paradigms. Advances in Intelligent Systems and Computing, vol 706. Springer, Singapore

- DOI (Digital Object Identifier) https://doi.org/10.1007/978-981-10-8237-5_9
- Publisher Name Springer, Singapore
- Print ISBN 978-981-10-8236-8
- Online ISBN 978-981-10-8237-5
- eBook Packages Engineering

Personalised recommendations