Asian Journal of Applied Science and Technology (AJAST)
(Open Access Quarterly International Journal) Volume 2, Issue 2, Pages 901-908, April-June 2018

Efficient Steganography in Encoded Video Streams Using Motion Vector Difference

C.B.Syamsudha[1] and S.Prabagar[2]

[1]*UG Student, Department of CSE, Excel Engineering College, Pallakapalayam, Tamilnadu, India.*
[2]*Assistant Professor, Department of CSE, Excel Engineering College, Pallakapalayam, Tamilnadu, India.*

Article Received: 27 January 2018 *Article Accepted: 23 February 2018* *Article Published: 23 May 2018*

ABSTRACT

The main purpose of this study is to explore secure data transmission with the video files. Generally, digital video sometimes are stored and processed in an encrypted format to maintain privacy and security. It is necessary to carry out data hiding operation with the encrypted videos. In such a way, in encrypted domain without decryption safeguard the confidentiality of the content through data hiding. In addition, it is more proficient without decryption followed by data thrashing and re-encryption. A new methodology of data hiding directly in the encrypted version of AVI video stream is proposed with this study. The approach is investigated with AVI video encryption (Triple DES), perturbation of data, embedding and extracting functionalities. The AVI file and the code words of motion vector differences are encrypted with streams. Finally, the sender may wish to embed additional data with encrypted data with codeword swap approach, without affecting the actual content of the motion picture files. Likewise, in the receiver side decryption operation and data extraction from the encrypted video files is carried out.

Keywords: Steganography and image processing.

1. INTRODUCTION

Image Processing is a technique to enhance raw images received from cameras/sensors placed on satellites, space probes and aircrafts or pictures taken in normal day-to- day life for various applications. Various techniques have been developed in Image Processing during the last four to five decades. Most of the techniques are developed for enhancing images obtained from unmanned spacecrafts, space probes and military reconnaissance flights. Image Processing systems are becoming popular due to easy availability of powerful personnel computers, large size memory devices and graphics software. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource.

2. LITERATURE REVIEW

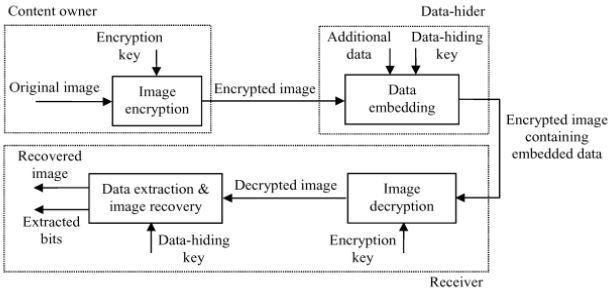
Bin Zhao [1] et al describe the most watermarking schemes for copyright protection, a seller usually embeds a watermark in multimedia content to identify a buyer. When an unauthorized copy is found by the seller, the traitor's identity can be traced by the embedded watermark. However, it incurs both repudiation issue and framing issue. To solve these problems, some buyer seller watermarking protocols have been proposed based on watermarking scheme in the encrypted domain. The enhanced scheme increases effective watermarking capacity, avoids additional overhead and overcomes an inherent defect that watermarking capacity depends on the probability distribution of input watermark sequence. Based on the security requirements of buyer–seller. Rini.J et al [6] describe the secure and authenticated discrete reversible data hiding in cipher images deals with security and

authentication. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. If the receiver has the encryption key, can decrypt the received data to obtain an image similar to the original one. If the receiver has both the data hiding key and the encryption key, can extract the additional data and recover the original content.

3. OVERVIEW OF THE STUDY

This thesis proposes a novel scheme for classic data hiding in encrypted images or video files. In the first phase, a content owner encrypts the original uncompressed image /video using an encryption key. Then, a data- hider may replace the least considerable bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image or video containing additional data, if a receiver has the data-hiding key, receiver can extract the additional data however user doesn't know the image content. If the receiver has the encryption key, then the receiver can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can pull out the additional data and recuperate the original content without any error by utilizing the spatial correlation in natural image when the amount of additional data is not too large.

4. ARCHITECTURE DIAGRAM



5. TECHNIQUES

The Motion Vector Difference (MVD) Encoding is carried out. In order to protect both texture information and motion information, not only the IPMs but also the motion vectors should be encoded. In avi file, motion vector prediction is further performed on the motion vectors, which yields motion vector difference. The values of motion vector difference are taken. For Data Embedding, in the encrypted bit stream of avi frames, the proposed data embedding is accomplished by substituting eligible codewords of various Levels. Since the sign of Levels are encrypted, data hiding should not affect the sign of Levels. For Data Extraction scheme, the hidden data can be extracted either in encrypted or decrypted domain. Data extraction process is fast and simple.

6. EXPERIMENTAL SETUP

6.1. Video File Selection:

In this phase, the video file selection is carried out open file dialog control and the path is displayed in text box and the video is displayed in media player control. Then the video file record is saved into 'Videos' table. The original video file selection is carried out and taken for Video Encryption. Then Encrypted Video is checked for playing in the player.

6.2. Perturbation of Input File:

In this phase, the text message is given as input. Two random characters are inserted between each two consecutive characters in the text message and the message is perturbated (confused).

Embedding the Encrypted Data:

In this phase, the text data is encrypted using TripleDES encryption and the bit sequences are taken for hiding. So, using the given data hiding key, the data embedding process is carried out with the given encrypted data. Finally, the encrypted data is made to hide inside the encrypted video.

Extraction of Encrypted Data and Decryption:

In this phase, the encrypted video with the hidden data is selected. For data extraction, Data-hiding key is given and the data is first extracted and then decrypted. Then with the video decryption key (same as encryption key), the video is decrypted and original video is obtained. The operation may be carried out in two types. A) First data extraction followed by Video decryption or B) Video decryption followed by data extraction.

7. ALGORITHMS

7.1. Parsing of Video

In this process, the frames are extracted from the submitted video file by means of sampling at regular interval out and extracted using AviFil32.dll methods. The frames are saved in a folder.

7.2. Perturbation

1. Text message or file is selected and submitted to the process.
2. Two random characters are inserted between each two consecutive characters in the text message and the message is perturbated (puzzled).

7.3. Encryption and Data Embedding

1. Text data from the file is selected
2. TripleDES encryption key is generated
3. For hiding, sequences of bit of the perturbated data is taken
4. Encoding the frame data from the processed video with dissimilar pixel values

5. Data embedding process is carried out with the given encrypted data using generated encryption keys
6. The encrypted data is embedded contained by the frames in the least significant bits

7.4. Data Extraction and Decryption

1. The encrypted video with the hidden data is selected
2. For data extraction, Data-hiding key is given and the data is first extracted and then decrypted
3. Then with the video decryption key (the key which is used for encryption), the video is decrypted and original video is obtained
4. Initially the data extraction followed by Video decryption or Video decryption followed by data extraction

8. EXPERIMENTAL RESULTS

First design a simplified mechanism to determine the number of neighboring nodes for any given node. Within time Tv, the given node crosses through an area and meets a number of neighbors N. Since mobile nodes are assumed uniformly distributed in the network, we may approximate N by

$$N = (\pi r^2 + 2rvT_v)\rho,$$

Where r denotes the transmission range of nodes, v is the velocity, and p is the density of nodes in the network. Based on the obtained number of neighboring nodes N, we can on firm the value of threshold K.

The following Table 6.1 describes experimental result for existing system secure transmission node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of send transmission node details are shown.

Table 6.1 LSB -Secure Transmission

S. NO.	NUMBER OF TIME SLOT (M)	RATIO OF SECURE TRANSMISSION NODE
1	10	0.43
2	20	0.52
3	40	0.61
4	60	0.69
5	80	0.74
6	100	0.80
7	120	0.86
8	140	0.90
9	150	0.93
10	160	0.97

The following Figure 6.1 describes experimental result for existing system secure transmission node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of send transmission node details are shown. The following Table 6.2 describes experimental result for proposed system secure transmission node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of send transmission node details are shown.

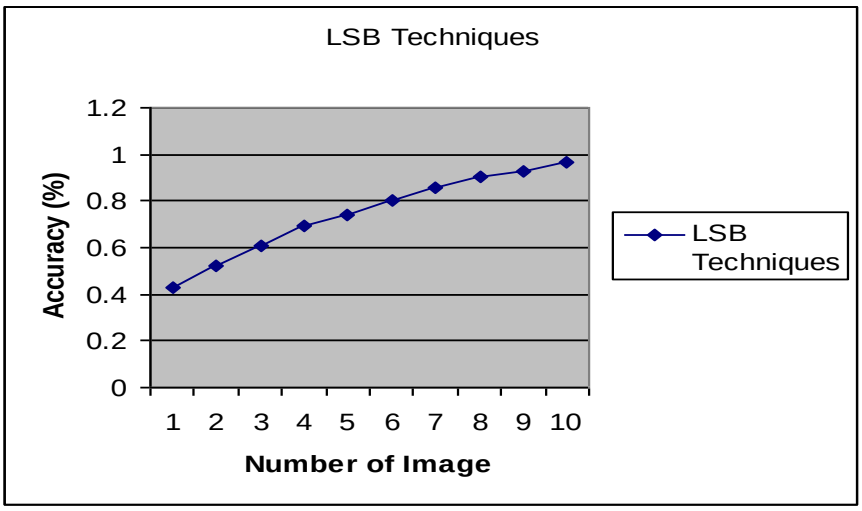


Fig 6.1 LSB Secure Transmission

Table 6.2 Code Word Secure Transmission

S.NO.	NUMBER OF TIME SLOT (M)	RATIO OF SECURE TRANSMISSION NODE
1	10	0.48
2	20	0.57
3	40	0.66
4	60	0.72
5	80	0.77
6	100	0.83
7	120	0.89
8	140	0.92
9	150	0.95
10	160	0.98

The following Figure 6.2 describes experimental result for proposed system secure transmission node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of send transmission node details are shown

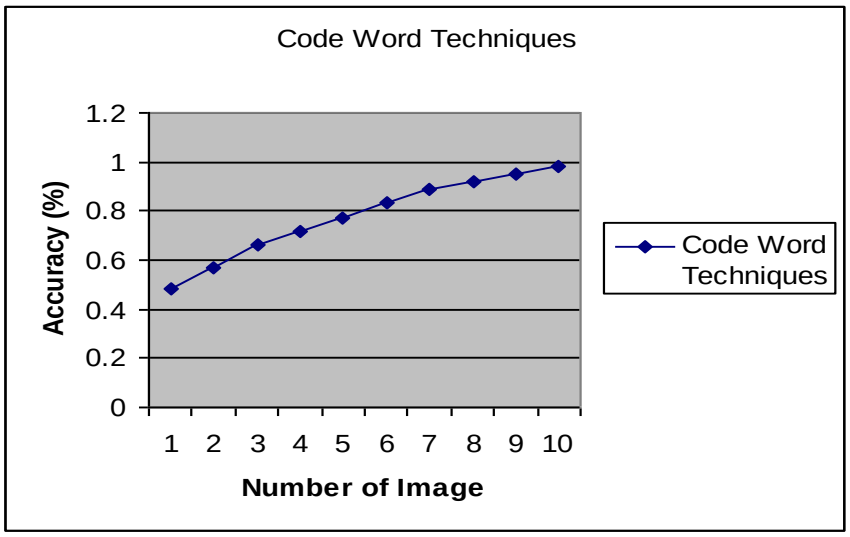
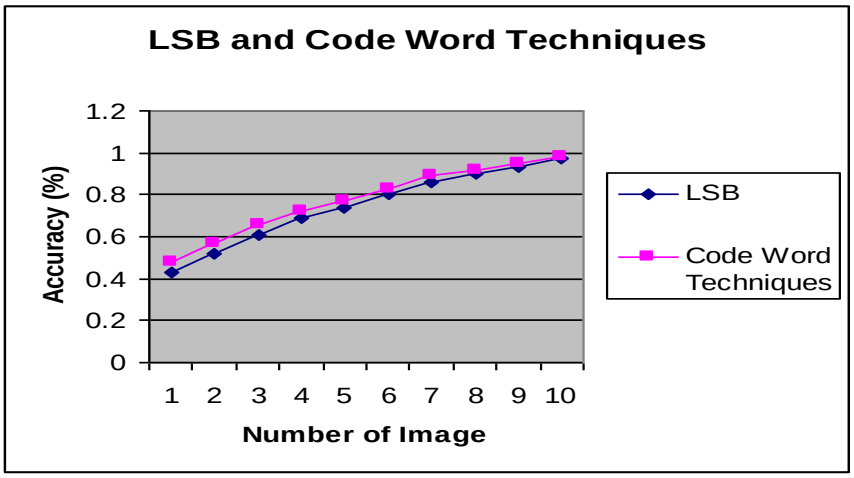


Fig 6.2 Code Word Secure Transmission

The following Figure 6.3 describe experimental result for differences existing system (LSB) and proposed system (Code Word) Secure transmission communication node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of send secure communication transmission node details are shown.

Table 6.3 Comparisons for SEEN and HASH Secure Transmission

S.NO.	NUMBER OF TIME SLOT (M)	RATIO OF SECURE TRANSMISSION NODE	
		LSB	Code Word
1	10	0.43	0.48
2	20	0.52	0.57
3	40	0.61	0.66
4	60	0.69	0.72
5	80	0.74	0.77
6	100	0.80	0.83
7	120	0.86	0.89
8	140	0.90	0.92
9	150	0.93	0.95
10	160	0.97	0.98



9. CONCLUSION

The data hiding in encrypted image is performed with this study. The approach is assessed with an applications substandard subordinate or a channel administrator hopes to tag on some bonus message, such as the foundation information, image notation or validation data, within the encrypted image though user does not know the original image content. And it is also expectant that the inventive content should be recovered without any blunder after image decryption and message pulling out at receiver side. The sender or owner of the encrypts the original image using an encryption key, and a data-hider can embed supplementary data into the encrypted image using a data-hiding key while the user does not know the actual content. With encrypted image containing additional data, the receiver may first decrypt it with the encryption key, and then extract the embedded data and recover the original image with the data-hiding key. In this scheme, the data extraction is not distinguishable from the content decryption. The complementary data should be hauling out from the decrypted image, so that the crucial content of original image is uncovered before data pulling out, and if someone has the data-hiding key but not the encryption key, they can't haul out any information from the encrypted image which containing additional data.

10. FUTURE WORKS

In this study, data hiding is completed entirely in the encrypted domain and the method can preserve the confidentiality of the content completely. With the encrypted video contains the hidden data, the data extraction can be carried out either in encrypted or decrypted domain. With this empirical study the avi file only is only taken for the data hiding process. Further different types of movie file formats can be taken for this process. Also, the data hiding process with no degradation in video quality is also needs to be considered.

REFERENCES

[1] B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," Inf. Sci., vol. 180, no. 23, pp. 4672–4684, 2010

[2] X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[3] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013

[4] V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," IEEE Trans. Multimedia, vol. 14, no. 3, pp. 703–716, Jun. 2012

[5] M. N. Asghar and M. Ghanbari, "An efficient security system for CABAC bin-strings of H.264/SVC," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 3, pp. 425–437, Mar. 2013.

[6] Yiqi Tew and Kok Sheik Wong, "An overview of Information Hiding in H.264/AVC Compressed Video", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 24, No. 2, pp. 305-319, 2014.

[7] Dawen Xu, Rangding Wang and Jicheng Wang, "A novel watermarking scheme for H.264/AVC video authentication", Signal Processing: Image Communication, Vol. 26, No. 6, pp. 267-279, 2011

[8] M. Noorkami and R. M. Mersereau, "A framework for robust watermarking of H.264-encoded video with controllable detection performance", IEEE Transactions on Information Forensics and Security, Vol. 2, No. 1, pp. 14-23, 2007.

[9] Jing Zhang, A. T. S. Ho, Gang Qiu and P. Marziliano, "Robust video watermarking of H.264/AVC", IEEE Transactions on Circuits and Systems II: Express Briefs, Vol. 54, No. 2, pp. 205-209, 2007.

[10] Mansouri, A. M. Aznaveh, Torkamani-Azar F and F. Kurugollu, "A Low Complexity Video Watermarking in H.264 Compressed Domain", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, pp. 649-657, 2010

[11] H. A. Aly, "Data hiding in motion vectors of compressed video based on their associated prediction error", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 1, pp. 14-18, 2011.

[12] Jian Li, Hongmei Liu, Jiwu Huang and Yun Q. Shi, "Reference index-based H.264 video watermarking scheme", ACM Transactions on Multimedia Computing, Communications, and Applications, Vol. 8, No. 2S, pp. 1-22, 2012.