International Journal of Digital Crime and Forensics
Volume 13 • Issue 4 • July-August 2021

An Intra-Prediction Mode-Based Video Steganography With Secure Strategy

Xiushi Cao, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

Tanfeng Sun, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

Xinghao Jiang, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

Yi Dong, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

Ke Xu, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

ABSTRACT

In this paper, an intra-prediction mode (IPM)-based video steganography with secure strategy was proposed for H.264 video stream. First of all, according to the property of IPM conversion after calibration, a content-adaptive selection strategy was adopted to measure candidate carrier macroblock. Then, a more efficient encoding strategy based on grouped IPM was applied to encode secret message. This encoding strategy aimed to further enhance the security performance by exploiting the deviation feature of calibrated IPM. Finally, syndrome-trellis code was used as the embedding implementation to minimize distortion. Experimental results demonstrate that this article proposed algorithm presents a novel security performance with any existing IPM-based video steganography.

KEYWORDS

Background-Subtraction, Content-Adaptive, H.264, Intra Prediction Mode, Secure Strategy, SVM, Syndrome-Trellis Code, Video Steganography

1. INTRODUCTION

As a new method to ensure communication security in the public network, Steganography technology has received more and more attention. Steganography is a technique for embedding secret information into an innocent-looking carrier. There are many medium that can be used as carrier, such as videos(Sadek, Khalifa, & Mostafa, 2015), audios(Dutta, Bhattacharyya, & Kim, 2009), images(Sharda & Budhiraja, 2013), et al. Video has become one of the most popular carrier for Steganography with the development of multimedia. Video Steganography can easily achieve a large Capacity with slight modification. H.264 is the most popular Video coding standard with higher compression efficiency(Kalva, 2006). In general, the well-established H.264 Video coding standard has adopted many advanced features, which can be exploited for Steganography.

Video Steganography (Liu, Liu, Wang, Zhao, & Liu, 2019) can be studied in many area, such as Motion Vector-based Steganography(Fan, Li, Yi, & Zhao, 2018; Li et al., 2019), Intra Prediction Mode(IPM)-based Steganography(Bouchama, Hamami, & Aliane, 2012; Xu, Wang, & Wang, 2012; Yang, Li, He, & Kang, 2011), variable length codes Stegangraphy(Lu, Chen, & Fan 2005; Seo, Choi, Lee, & Kim, 2008) and quantized Discrete Cosine Transform(DCT) coefficient-based Steganography(Cao, Wang, Zhao, Zhu, & Xu, 2018; Mstafa,Elleithy, &Abdelfattah, 2017). IPM-

DOI: 10.4018/IJDCF.20210701.oa1

This article, published as an Open Access article on June 4th, 2021 in the gold Open Access journal, the International Journal of Digital Crime and Forensics (converted to gold Open Access January 1st, 2021), is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

based Steganography is motivating because it can well preserve the quality of the Video. IPM-based Steganography has been studied in many years. Xu et al.(2012) simply modulate the IPM of qualified Intra 4x4 blocks to embed secret message. Yang et al.(2011) introduce Matrix coding to increase the Capacity by hiding two bits information by modifying one IPM. Bouchama et al.(2012) further enhance Capacity by grouping the IPM to minimize the distortion brought by IPM modification. In these methods, the modulation of IPM inevitably destroy the optimal selection rule of IPM, which can be easily detected by Intra Prediction Mode Calibration(IPMC) (Zhao, Zhang, Wang, & Zhao, 2015) steganalytic method. In order to resist against IPMC, Nie et al. (2018) apply Syndrome-Trellis Code(STC) (Filler, Judas, & Fridrich, 2011) with a designed distortion function based on Sum of Absolute Deviations(SAD) prediction deviation to IPM-based Steganography and the algorithm achieve large increase in security performance. After analysing the features used in IPMC, it can observed that the performance of IPMC is related to the Video content. However, there was no existing IPM Steganography which exploit the characteristics of Video content.

In order to make full use of the characteristics of carrier Video, this paper proposed a novel secure Video Steganography with a content-adaptive candidate macroblocks selection strategy. Background subtraction algorithm was applied to select the foreground blocks as the Candidate carrier macroblocks. To further improve the security performance in resisting against IPMC, a more efficient encoding strategy based on grouped IPM was applied to encode the secret message.

The rest of this paper is organized as follows. In Section 2, H.264 Intra Prediction and the previous work of Intra Prediction Mode Steganography is introduced. In Section 3, IPMC is analyzed to find out the opportunity to confuse the Steganalysis algorithm. The proposed secure strategy is elaborated in Section 4 and the framework of proposed algorithm is given in Section 5. The experimental evaluation is shown in Section 6. In the end, conclusions and future works are given in Section 7.

2. PRELIMINARIES

In this section, H.264 Intra Prediction is first presented. Then, the previous work of Intra Prediction Mode Steganography is briefly introduced.

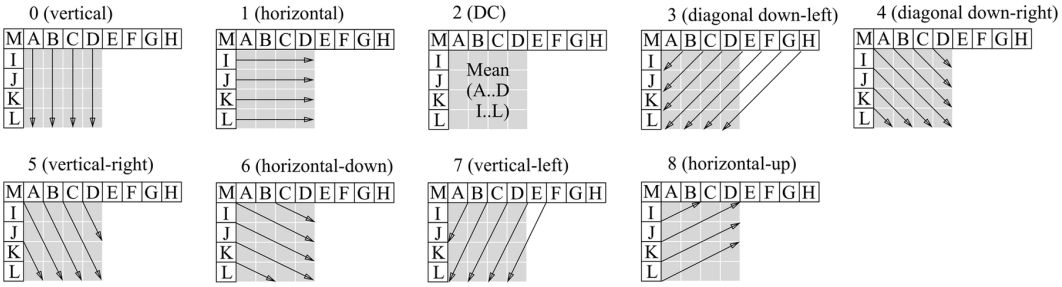
2.1 H.264 Intra Prediction

In H.264 Intra Prediction, spatial redundancy was exploited to compress Video content(Wiegand, Sullivan, Bjontegaard, & Luthra, 2003; Sofokleous, 2005). The principle is that the pixel value of adjacent macroblock are relatively close. The encoder use previously encoded pixel value and reconstructed neighbor macroblocks as the reference to predict the pixel value of current macroblock. The difference between the predicted pixel value and the original pixel value was additionally encoded and represented with a reduced number of bits compared to the original pixel value.

There are 9 prediction direction in intra 4x4 luma macroblock, and 4 predicting direction in intra 16x16 luma macroblock. The intra 4x4 prediction modes are more convenient for areas of significant details and the intra 16x16 prediction modes are more suitable for smooth area. Most of the time, Video has only a few of intra 16x16 prediction modes, and intra 16x16 modes are not worth exploiting because human eye are sensitive to notice the modification. The 9 predicting direction of intra 4x4 luma macroblock is given in Figure 1.

As shown in Figure 1, pixels A~M are the already encoded boundary pixels which will be used as the reference to predict 4x4 macroblock pixel value. The weighting calculation of reference pixels A~M is carried out according to different prediction direction, such as DC mode, using (A+B+C+D+I+J+K+L) / 8 as the predicted pixel value. To take full advantage of the properties of intra-prediction, for each macroblock, all the available IPM are performed and calculated with the encoding cost, respectively. Then, the encoder follow the optimal selection rule to choose the IPM with the smallest cost.

Figure 1. Prediction direction of intra 4×4 luma macroblock



2.2 The Previous Work of Intra Prediction Mode-Based Steganography

Calibration-base steganalysis (Fridrich & Kodovsky, 2012; Cao, Zhao, & Feng, 2012) had achieved high detection accuracy in the last few years. Firstly, these methods reconstruct an estimation of the cover from the Steganography Video. Then, features based on the difference between the estimated cover and origin Video are extracted. Finally, classifier, such as SVM et al., is trained with these features to make classification. For Intra Prediction Mode Steganalysis, Zhao et al. (2015) proposed the IPMC features based on the calibration method, which is sensitive to the non-optimal IPMs.

In order to resist against IPMC, Nie et al. (2018) find out the fact that the Intra Prediction Mode reversion phenomenon is mainly caused by increasing the SAD (Kim & Jeong, 2012) value. Thus, the authors proposed the Sum of Absolute Deviations(SAD) prediction deviation(SPD) as the distortion function to minimize the SAD lift brought by modulate IPM. SAD is the rough estimation cost of encoding macroblock and SAPD is the prediction deviation, these formulas is given below.

$$SAD_{i,t} = \sum_{(x,y)\in B_{i,t}} \left| O_{i,t}\left(x,y\right) - R_{i,t}\left(x,y\right) \right| \tag{1}$$

$$SPD_{i,t} = \left| SAD_{i,t}\left(m_{i,t}\right) - SAD_{i,t}\left(m'_{i,t}\right) \right| \tag{2}$$

where B is the current macroblock, $O_{i,t}\left(x,y\right)$ represents the origin pixel value and $R_{i,t}\left(x,y\right)$ is the reconstructed pixel value carried out by prediction direction, $SAD_{i,t}\left(m_{i,t}\right)$ is the prediction SAD of the optimal mode $m_{i,t}$ associated with the i-th prediction block in the t-th I-frame.

With the SAD prediction deviation, 9 Intra Prediction Modes is grouped and IPM can not be modulated to each other in the same group. The authors put the modes with large SPD into the same group to reduce the probability of significantly increasing the distortion caused by modulating IPM. Further more, ± 1 STC is used as the practical steganographic method for secret message embedding and extraction.

The method can well resist steganalysis as it target to overcome the defect of modulation IPM. However, the study of IPMC is insufficient, it still has more space to enlarge the security performance.

3. ANALYSIS OF IPMC STEGANALYTIC METHOD

In IPM-based Steganography, secret message is embedded by modulating IPM. As mentioned above, the modification of IPM inevitably destroy the optimal selection rule of IPM, and these phenomena are used as the clue by steganalytic algorithm to diverse Steganography Video and non-Steganography Video. According to this observation, the recently proposed Intra Prediction Mode Calibration(Zhao, Zhang, Wang, & Zhao, 2015) method had achieved the most effective detection performance against the IPM-based Video Steganography. In this section, IPMC is studied in order to propose effective strategy to resist against it.

3.1 Intra Prediction Mode Conversion after Calibration

In IPMC, every Intra 4x4 macroblock is decompressed and compressed again to reselect IPM and save relevant information. IPM in cover Video will remain unchanged after Calibration at utmost degree, while altered IPM is very likely to revert to their prior optimal value in Steganography Video. IPMC use the differences of IPM before and after Calibration as the main clue to distinguish Steganography Video. However, IPM in cover Video will sometimes convert after Calibration. These conversion have been studied in this paper. Eight Video sequences were used to extract the IPM after Calibration. IPM Conversion Rate(CR) is calculated as

$$CR = \frac{\sum_{k=1}^{L}\sum_{n=1}^{M_k}\delta\left(I_{k,n},\hat{I}_{k,n}\right)}{\sum_{k=1}^{L}M_k} \tag{3}$$

$$\delta\left(I_{k,n,},\hat{k},n\right) = \begin{cases} 1 & I_{k,n} = \hat{I}_{k,n} \\ 0 & I_{k,n} \neq \hat{I}_{k,n} \end{cases} \tag{4}$$

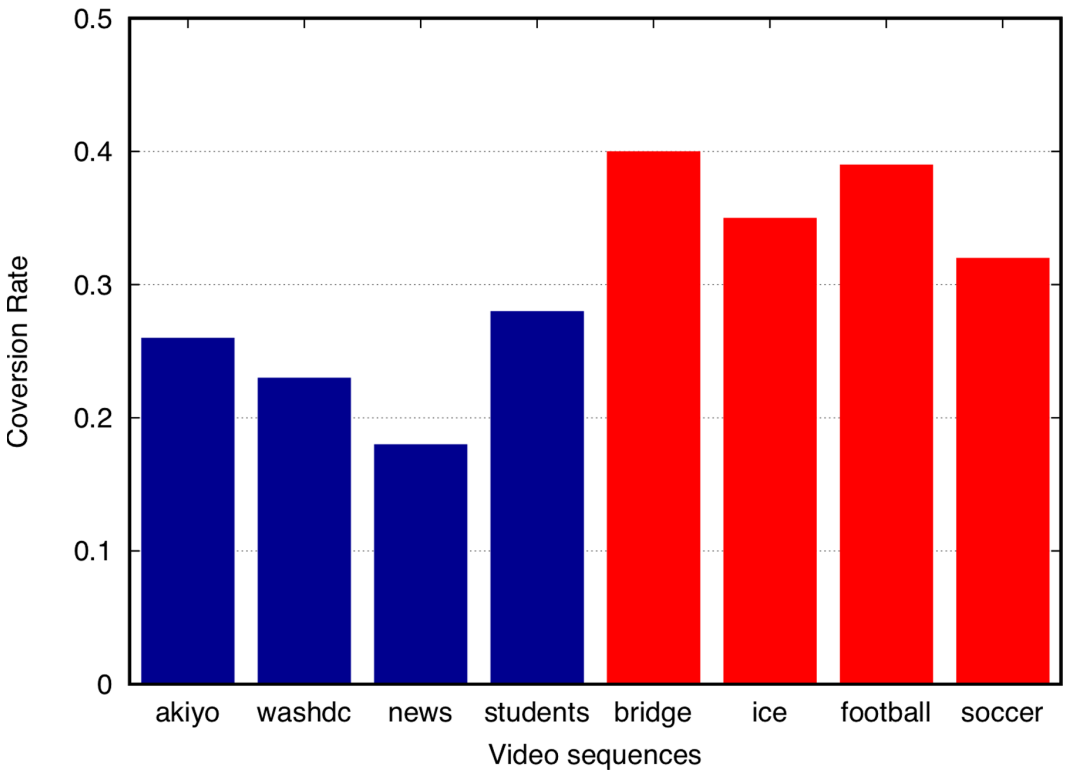
where L is the number of I-frame, and $\boldsymbol{M_k}$ is the number of IPM in k frame. $\boldsymbol{I_{k,n}}$ is the origin IPM, and $\hat{\boldsymbol{I}}_{\boldsymbol{k,n}}$ is the IPM after Calibration. The statistics is shown in Figure 2.

It can be observed from Figure 2 that the Conversion Rate in different cover Video varies large. The static content Video(the first four Video sequences) tend to have low Conversion Rate and the dynamic content Video(the last four Video sequences) are more likely to convert IPM after Calibration. The optimal IPM with minimum cost is selected in Calibration procedure, IPM conversion means that the cost performed by original IPM is not the minimum.

In H.264 standard, Rate-Distortion(RD) cost function is recommended as the cost function. The control model based on Lagrangian optimization algorithm is used to achieve the choice of optimal IPM. However, the computational complexity of RD cost function is quite high. In practical, the H.264 standard use Sum of Absolute Transformed Differences(SATD)(Kim & Jeong, 2012) as the cost function to select optimal IPM, and the IPM with the minimum SATD is selected. SATD is calculated based on the differences between the original pixel value and the predicted pixel value.

$$SATD = \sum_{(x,y)}\left|H\left(P\left(x,y\right) - P_{predicted}\left(x,y\right)\right)\right| \tag{5}$$

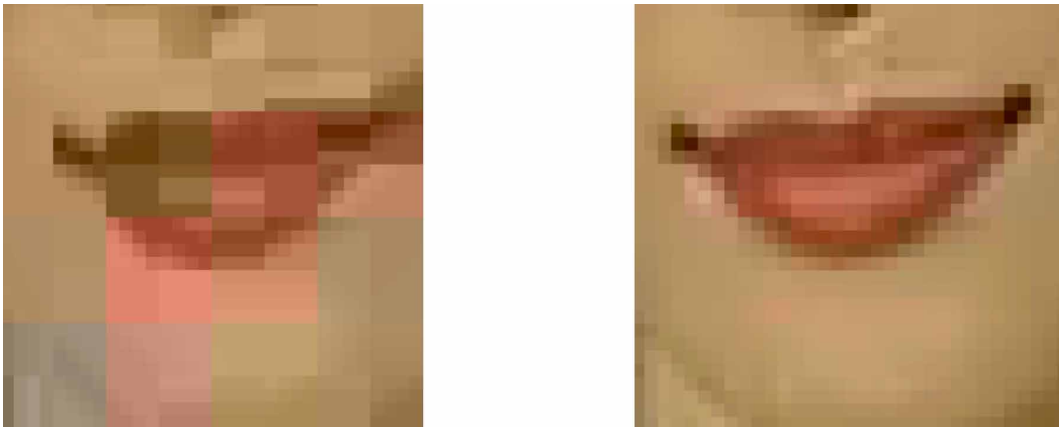
Figure 2. IPM Conversion Rate after Calibration



where $H\left(\cdot\right)$ represents the Hadamard transform. $P\left(\cdot\right)$ represents the original pixel value. $P_{predicted}\left(\cdot\right)$ represents the predicted pixel value.

The differences between predicted block and original block is shown in Figure 3. It can be seen that the predicted block is smooth. In Steganography, IPM is modulated to embed secret message, and the modulated IPM causes impact with the pixel value in predicted block. According to Equation

Figure 3. Predicted block and original block of mouth



(5), the SATD in smooth block is more likely to have a large distortion after IPM modulation because the pixel value is closely correlated to the predicted block, and the SATD of complex texture block is less sensitive to the modulation of IPM. As discussed above, IPM in block with diverse pixel value is more likely to transform to other IPM after Calibration for the reason that the predicted block performed by IPM contributes less to SATD.

In short, it can be concluded that the IPM in dynamic block is more suitable to be chose as the carrier to embed secret message.

3.2 Intra Prediction Mode Transformation After Calibration

According to above analysis, IPM in dynamic content Video is more likely to transform to another IPM after Calibration. These transformation was studied in this section. The cover Video was decoded and encoded again to obtain the IPM after Calibration. Every IPM transformation after Calibration was saving and the feature IPM Transformation Probability(TPR) is calculated as below.

$$TPR_{org}^{c} = \frac{\sum_{k=1}^{L} \sum_{i=1}^{U_{org,k}} \delta\left(c, \hat{I}_{k,i}\right)}{\sum_{k=1}^{L} U_{org,k}} \tag{6}$$

$$\delta\left(c, \hat{I}_{k,i}\right) = \begin{cases} 1 & c = \hat{I}_{k,i} \\ 0 & c \neq \hat{I}_{k,i} \end{cases} \tag{7}$$

where $org \in [0,8]$ is the original IPM, $\boldsymbol{c} \in [0,8]$ is the Calibrated IPM, and $\hat{I}_{k,i} \in [0,8]$ is the Calibrated IPM of i-th org IPM in kth I-frame. $U_{org,k}$ is the total number of org IPM in k-th I-frame.

It can be seen from Figure 4 that every IPM has intended IPM to transform after Calibration. It can be assumed that if the IPM modulation follows the transform intention, the IPM difference in Steganography Video after Calibration will be similar to the IPM difference in cover Video.

In short, the transformation intention of IPM in cover Video can be used as the guide to group IPM, the IPM modulation in the same group is less likely to be distinguished by IPMC because of the similarity to cover Video.

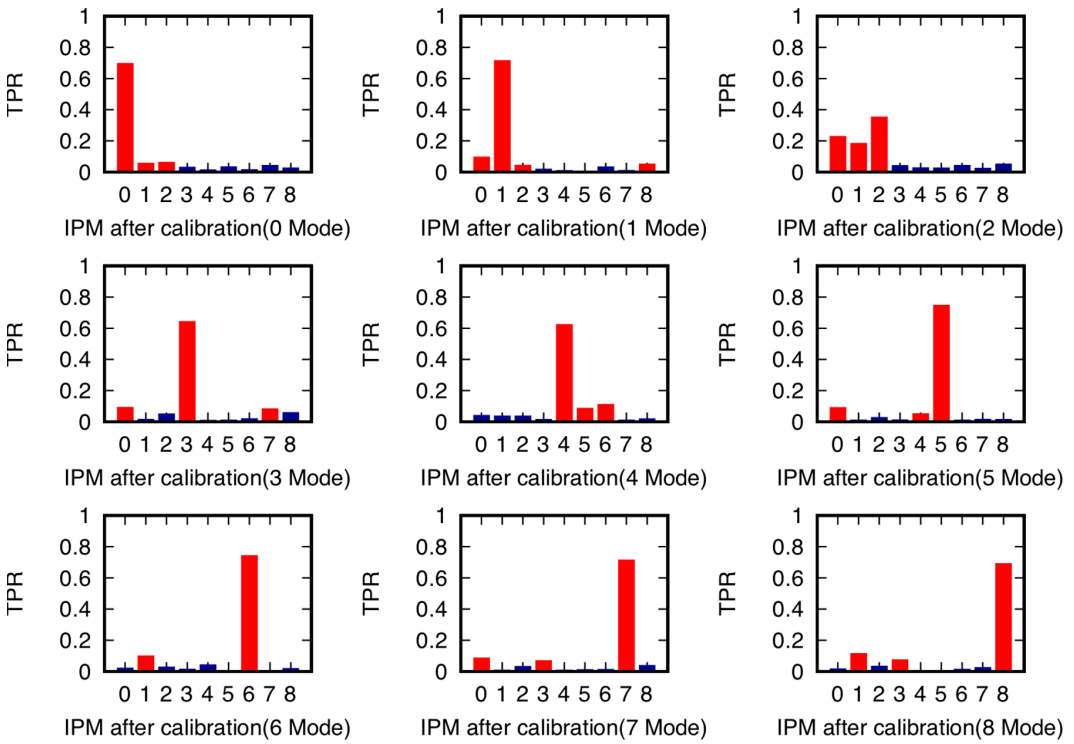
4 PROPOSED STRATEGY AGAINST IPMC

4.1 Content-Adaptive Selection Strategy

Most of the IPM-based Steganography use all of the available Intra 4x4 macroblocks as the candidate carrier. The Capacity is maximized in this way, but the security is tending to low because some macroblocks are unsuitable for embedding message. Once these macroblocks have been modified, it is very likely to revert to the original IPM after Calibration utmost time. According to Section 2, the static background content macroblock with low IPM conversion rate are not suitable for embedding message.

Therefore, the principle for selecting candidate macroblock is to skip static background macroblock and only the dynamic front macroblock is preserved as the candidate carrier. In the proposed strategy, background subtraction is used to separate “foreground” and “background” in Video sequences, and “foreground” block is used as the mask to guide the selection procedure.

Figure 4. IPM Transformation Probability after Calibration



4.2 Encoding Strategy

According to Section 2, IPM Transformation Probability was studied to figure out the IPM transformation phenomenon after Calibration. Every IPM has their preferable IPM, and it's obviously that if the modulation of IPM follows the same behavior like this, IPMC will be effectless to distinguish cover Video and Steganography Video. With the knowledge of that, the proposed encoding strategy can be designed and the strategy consists of two parts, the group method and mapping rule. The group method is shown in Table 1.

In Table 1, m represents original IPM, m' represents modulated IPM. 1 means that these two modes are in the same group and this modulation is allowed and. For example, according the prediction mode 0 row, prediction mode 2 column is 1 means that mode 0 can be modulated to mode 1. In the same way, mode 0 can't be modulated to mode 3 as the mode 3 column of mode 0 row is 0.

The mapping rule(Cao, Zhou, & Sun, 2018) are decided based on the group method. As discussed above, mode is allowed to be modulated to another same group mode. IPM in the same group are divided into two parts, one part for bit message 0 and another for bit message 1. Table 2 shows the mapping rule.

The overall encoding rule is given in Figure 5. Every IPM is mapped to bit message 0 or bit message 1 according to the mapping rule, and the original IPM can be modulated to the same group IPM with different bit message. For example, suppose that the original IPM is 1, the bit message is 0 according to the mapping rule and it can be modulated to IPM 2 if the corresponding bit message is 1.

Table 1. Group method

m' / m	0	1	2	3	4	5	6	7	8
0	0	0	1	0	0	0	0	0	0
1	0	0	1	0	0	0	0	0	1
2	1	1	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0	1	0
4	0	0	0	0	0	1	0	0	0
5	1	0	0	0	1	0	1	0	0
6	0	1	0	0	0	1	0	0	0
7	1	0	0	1	0	0	0	0	0
8	0	1	0	0	0	0	0	0	0

5 PRACTIAL IMPLEMENTATION

The framework of proposed algorithm is shown in Figure 6. The proposed algorithm can be implemented as follows.

Generate Front Block Masks: Only "foreground" block will be used to embed secret message, thus the first step is generate front block mask to select "foreground" block. Original YUV Video is used directly to feed background subtraction algorithm, colored "foreground" segmentation frame can be produced after the processing. Then, every frame is partitioned into l6x16 block which is similar to H.264 luma macroblocks. Also, a threshold is set to judge which block is "foreground", the "foreground" block is defined as the block which have enough colored part and can meets threshold. After calculation, front block mask is got and it will be used in subsequent step.

Obtain original IPM and SATD: In order to obtain the original IPM, the YUV Video sequences need to go through a dummy encoding process with H.264 encoder. In this procedure, the encoded Video will not be used, the most important thing is that the IPM and SATD is extracted and saved in this procedure. Macroblock number and position is also need to be saved as to extract front

Table 2. Mapping rule

IPM	Prediction Direction	Bit Message
0	Vertical	0
1	Horizontal	0
2	DC	1
3	Diagonal Down-Left	0
4	Diagonal Down-Righ	0
5	Vertical-Right	1
6	Horizontal-Down	0
7	Vertical-Left	1
8	Horizontal-Up	1

Figure 5. Encoding strategy

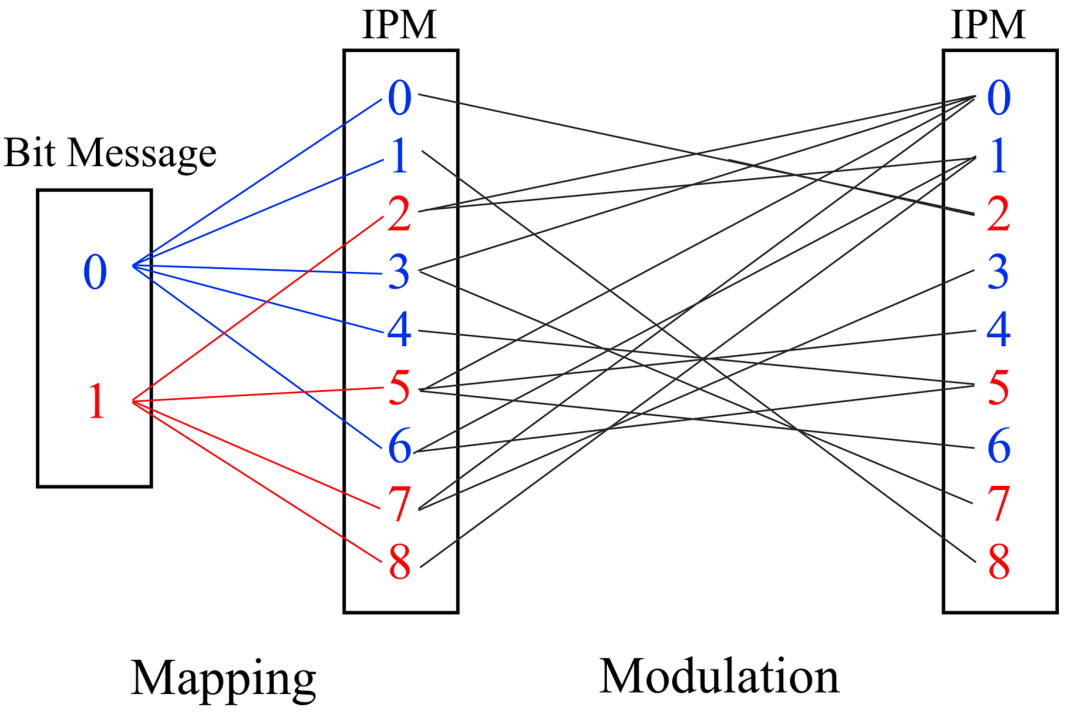
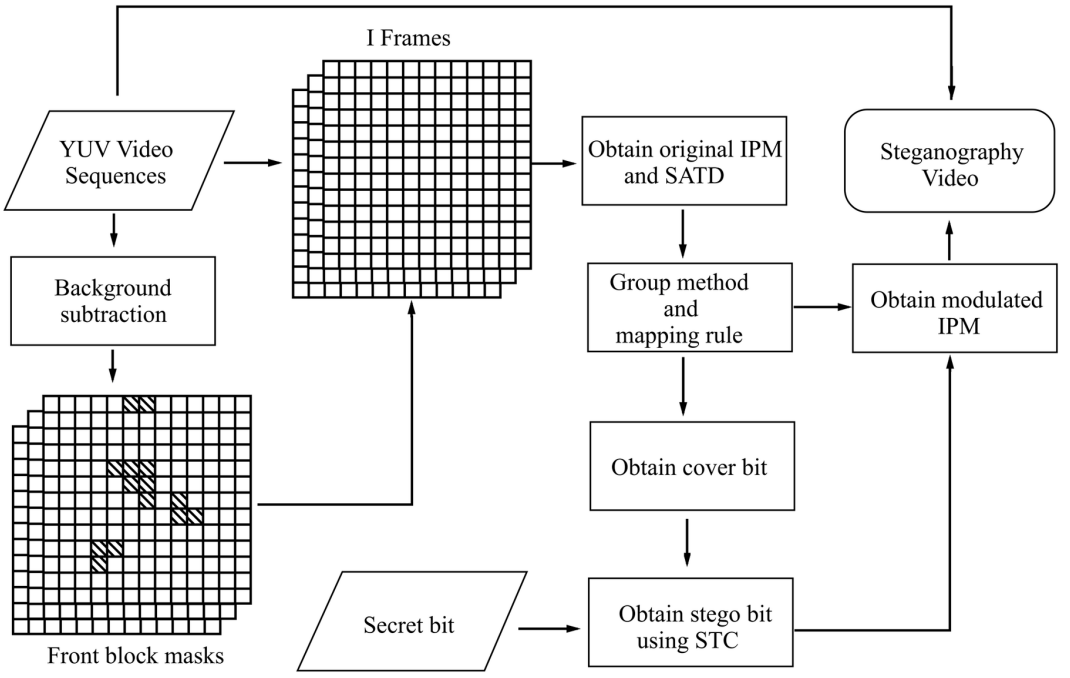


Figure 6. Framework of proposed algorithm



macroblocks. With these position information and pre-generated front block masks, front macroblocks and corresponding IPM and STAD can be obtained with calculation.

Obtain Cover Bit: Cover bit message can obtained from the original IPM, every mode can be represented as a bit message according to the mapping rule.

Obtain Stego Bit: First of all, secret message is encoded to secret bit which is constructed by bit 0 and bit I. Then, cover bit and secret bit is prepared for STC embedding, STC is the embedding method which can minimize the distortion function, the distortion function used here is the pre-save SATD value extracted from first step. The reason why SATD is used as the distortion function is that the smaller the SATD is, the less probability that this modulation can be analyzed by IPMC as discussed above.

Obtain Modulated IPM: Cover bit is generated from original IPM, and stego bit is the ideal bit that can be extracted to reproduce secret message. In order to hide the secret message in Cover Video, the IPM need to be modulated to corresponding IPM which can mapped to ideal bit. The process can be operated bit by bit, there are two situation here. One for the stego bit is the same as the cover bit and there are no need to make the IPM modulation. Another one is that the stego bit doesn't meet the cover bit, in this case the origin IPM need to be modulated to the same group IPM which has a different mapped bit message. For example, the original IPM is 1 and the corresponding cover bit is 0, however the stego bit is 1 after STC embedding. In order to hide the secret message, the origin IPM can be modulated to mode 2 or mode 8 according to the group method and mapping rule, the final choice of mode 2 or mode 8 is determined by the SATD. The mode with smaller SATD will be chose as the target mode to be modulated.

Encode YUV Video sequences: The final step is to encode the YUV Video sequences with the modulated IPM. In the general H.264 encoding procedure, all the available IPM are performed and calculated with the encoding cost, the encoder will follow the optimal selection rule to choose the IPM with the smallest cost. In the proposed algorithm, the modulated IPM will be chose as the IPM to be encoded.

6 EXPERIMENT

6.1 Experiment Setup

A Video database consisting of 33 standard test sequences downloaded from the Internet is used for experiments. All Video sequences are stored in 4:2:0 YUV format and have the size of CIF (352×288). The original Video sequences have various scenes and various frames (mostly 300 frames). The maximum interval between I frame(IDR) is set with 10 to ensure the number of I-frame samples. In order to maximum the performance of the background subtraction algorithm, which built model based on consecutive frames, original Video is used directly. The proposed algorithm is implemented on a well-known H.264 codec named x264. The practical background subtraction algorithm is proposed by Godbehere, etc al.(2012) Syndrome-Trellis Codes Toolbox was used as the STC embedder. LibSVM toolbox(Chang & Lin, 2011) with the polynomial kernel is employed for classification. Nie's algorithm is also implemented to compare the performance (Table 3).

6.2 Analysis of Security Performance

The security performance of steganographic algorithm is the most important indicator. The state of the art steganalytic algorithm IPMC(Zhao et al., 2015) is used to measure the security performance.

In the test, 80% Video sequences are randomly selected for training, and the remaining 20% Video sequences are used for testing. The experiment was repeated 10 times to calculate the average detection Error Probability(P_E). In order to compare the security performance of algorithm in different Video quality and STC Payload, 1 Mb/s bit rate and 0.5 Mb/s bit rate was used, and the STC Payload was range from 0.125 to 0.5.

Table 3. Experimental Parameter

Number of Video	33
Video Format	4:2:0 YUV
Video Size	CIF(352×288)
IDR	10
Bit Rate	{0.5, 1} Mb/s

$$P_E = \frac{FP + FN}{TP + FP + TN + FN} \tag{8}$$

where TP, TF, FP, FN is the detection result of IPMC. The theoretical maximum value of P_E is 0.5 which means the IPMC algorithm nearly make a random guess.

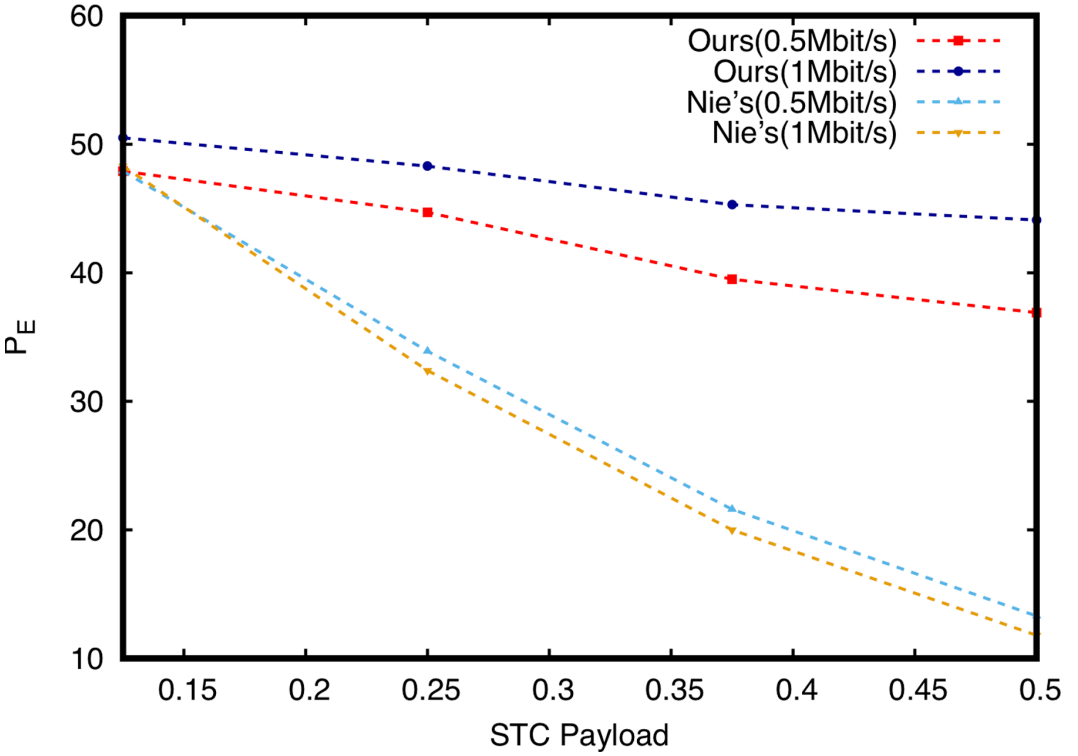
The security performance of these two algorithms are shown in Table 4 and Figure 7.

The P_E of Nie's algorithm and the proposed algorithm is shown in Table 4. It can seen that the P_E with 1Mbit/s bit rate and 0.5 STC Payload of the proposed algorithm is 44.1, which is far more large than Nie's 11.8. The result shows that the proposed algorithm has better security performance than Nie's. Besides, it can be seen that most of the P_E of proposed algorithm is close to 0.5, which

Table 4. Comparsion of security performance

Algorithm	Bit Rate (Mb/s)	STC Payload	P_E (%)
Nie's	0.5	0.125	47.9
		0.25	33.9
		0.375	21.6
		0.5	11.3
	1	0.125	48.3
		0.25	32.4
		0.375	20.0
		0.5	11.8
This Article's	0.5	0.125	47.9
		0.25	44.7
		0.375	39.5
		0.5	36.9
	1	0.125	50.5
		0.25	48.3
		0.375	45.3
		0.5	44.1

Figure 7. Comparsion of security performance



is the theoretical maximum value of P_E. It can be concluded that IPMC almost have no effect in classifying the Steganography Video modulated by the proposed algorithm.

The security performance of Nie's algorithm and the proposed algorithm is compared in Figure 7. As shown in Figure 7, the P_E curve of the proposed algorithm is higher than Nie's regardless of bit rate and STC Payload, which represents the proposed algorithm has a better security performance than Nie's in resisting against IPMC. Additionally, it can be observed that the P_E curve of the proposed algorithm is smoother than Nie's, which can be explained that the security performance of the proposed algorithm is less likely to be influenced by the size of embedded secret message. Except the novel security performance compared with Nie's algorithm, the proposed algorithm performs better in high bit rate. The main reason of that is the introduction of background subtraction method. High bit-rate Video preserve the quality of Video, which maintain significant detail in complex texture blocks, and these blocks are the best carrier to be modulated to embed secret message.

Above all, it can be concluded from the experiment results that the proposed algorithm achieves a novel performance in resisting against IPMC.

6.3 Analysis of Video Quality

Peak Signal-to-Noise Ratio (PSNR) is the measurement commonly adopted to judge Video quality in steganographic algorithm. In order to measure the quality influence brought by steganographic algorithm, PSNR of cover Video is also given.

Three Video sequences "Costguard.yuv", "Mobile.yuv" and "Waterfall.yuv" were tested and the results are shown in Table 5.

Table 5. Comparsion of video quality

Video Sequences	Bit Rate (Mb/s)	Cover	Nie's	This Article's
Costguard.yuv	0.5	31.06	30.92	31.04
	1	34.78	34.72	34.76
Mobile.yuv	0.5	30.58	30.49	30.56
	1	32.92	32.90	32.91
Waterfall.yuv	0.5	32.22	32.14	32.22
	1	35.47	35.43	35.46

As expected, with the introduction of the content-adaptive selection rule which skip static content macroblock to avoid the significant quality decrease inflected by IPM modulation, the proposed embedding algorithm actually maintain the Video quality very well and the modulation to cover Video is nearly to be invisible.

Above all, it can be concluded from the experimental results that the proposed algorithm has few impact on visual quality for Video stream.

7. CONCLUSION

In this paper, a novel secure Video Steganography with a content-adaptive candidate marcoblock selection strategy was proposed. Besides, a more efficient encoding strategy based on grouped IPM was applied to further enhance the security performance. Although the Capacity is damaged because of some unsuitable macroblocks are skipped to embed message, the proposed method achieves a better performance in security. In future work, there is still room for improvement on the candidate macroblock selection strategy.

ACKNOWLEDGMENT

This work is funded by National Natural Science Foundation of China (Grant No.61572320). It is also supported by National Key Research and Development Projects of China (2018YFC0830700, 2018YFC0831405) and the Fundamental Research Funds for the Central Universities. The corresponding author is Dr. Tanfeng Sun.

REFERENCES

Bouchama, S., Hamami, L., & Aliane, H. (2012). H.264/avc data hiding based on Intra prediction modes for real-time applications. *Lecture Notes in Engineering and ComputerScience*, *2200*(1), 655–659.

Cao, Y., Wang, Y., Zhao, X., Zhu, M., & Xu, Z. (2018). Cover Block Decoupling for Content-Adaptive H.264 Steganography. *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '18),* 23-30.

Cao, Y., Zhao, X., & Feng, D. (2012). Video steganalysis exploiting motion vector reversion-based features. *IEEE Signal Processing Letters*, *19*(1), 35–38. doi:10.1109/LSP.2011.2176116

Cao, Y., Zhou, Z., & Sun, X. (2018). Coverless information hiding based on the molecular structure images of material. Computers. *Materials & Continua*, *54*(2), 197–207.

Chang, C. C., & Lin, C. J. (2011). Libsvm: A library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, *2*(27), 1–27. doi:10.1145/1961189.1961199

Dutta, P., Bhattacharyya, D., & Kim, T. (2009). Data Hiding in Audio Signal: A Review. *International Journal of Database Theory and Application*, *2*(2), 1–8.

Fan, X., Li, H., Yi, J., & Zhao, X. (2018). Motion Estimation Steganography Based on H.264. *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, 249-254.

Filler, T., Judas, J., & Fridrich, J. (2011). Minimizing additive distortion in Steganography using syndrome-trellis codes. *IEEE Transactions on Information Forensics and Security*, *6*(3), 920–935. doi:10.1109/TIFS.2011.2134094

Fridrich, J., & Kodovsky, J. (2012). Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, *7*(3), 868–882. doi:10.1109/TIFS.2012.2190402

Godbehere, A. B., Matsukawa, A., & Goldberg, K. (2012). Visual tracking of human visitors under variable-lighting conditions for a responsive audio art installation. *2012 American Control Conference (ACC)*, 4305-4312. doi:10.1109/ACC.2012.6315174

Kalva, H. (2006). The H.264 Video Coding Standard. *IEEE MultiMedia*, *13*(4), 86–90. doi:10.1109/MMUL.2006.93

Kim, J., & Jeong, J. (2012). Fast intra mode decision algorithm using the sum of absolute transformed differences. *International Conference on Digital Image Computing Techniques and Applications*, 655-659.

Li, D., Zhang, Y., Li, X., Niu, K., Yang, X., & Sun, Y. (2019). Two-dimensional histogram modification based reversible data hiding using motion vector for H.264. *Multimedia Tools and Applications*, *78*(7), 8167–8181. doi:10.1007/s11042-018-6729-3

Liu, Y., Liu, S., Wang, Y., Zhao, H., & Liu, S. (2019). Video steganography: A review. *Neurocomputing*, *335*, 238–250. doi:10.1016/j.neucom.2018.09.091

Lu, C., Chen, J., & Fan, K. (2005). Real-time frame-dependent video watermarking in VLC domain. *Signal Processing Image Communication*, *20*(7), 624–642. doi:10.1016/j.image.2005.03.012

Mstafa, R. J., Elleithy, K. M., & Abdelfattah, E. (2017). A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC. *IEEE Access: Practical Innovations, Open Solutions*, *5*, 5354–5365. doi:10.1109/ACCESS.2017.2691581

Nie, Q., & Xu, X. (2018). Defining Embedding Distortion for Intra Prediction Mode-Based Video Steganography. *CMC: Computers, Materials & Continua, 55*(1), 59-70.

Sadek, M., Khalifa, A., & Mostafa, G. (2015). Video steganography: A comprehensive review. *Multimedia Tools and Applications*, *74*(14), 7063–7094. doi:10.1007/s11042-014-1952-z

Seo, Y., Choi, H., Lee, C., & Kim, D. (2008). Low-complexity watermarking based on entropy coding in H.264/AVC. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, *91*(8), 2130–2137. doi:10.1093/ietfec/e91-a.8.2130

Sharda, S., & Budhiraja, S. (2013). Image Steganography: A Review. *International Journal of Emerging Technology and Advanced Engineering*, *3*(1), 707–710.

Sofokleous, A. (2005). Review: h.264 and mpeg-4 video compression: video coding for next-generation multim edia. *The Computer Journal*, *48*(5), 563–563. doi:10.1093/comjnl/bxh117

Wiegand, T., Sullivan, G. J., Bjontegaard, G., & Luthra, A. (2003). Overview of the h.264/avc video coding standard. *IEEE Transactions on Circuits and Systems for Video Technology*, *13*(7), 560–576. doi:10.1109/TCSVT.2003.815165

Xu, D., Wang, R., & Wang, J. (2012). Prediction mode modulated data-hiding algorithm for h.264/avc. *Journal of Real-Time Image Processing*, *7*(4), 205–214. doi:10.1007/s11554-010-0175-4

Yang, G., Li, J., He, Y., & Kang, Z. (2011). An information hiding algorithm based on Intra-prediction modes and matrix coding for h.264/avc Video stream. *International Journal of Electronics and Communications*, *65*(4), 331–337. doi:10.1016/j.aeue.2010.03.011

Zhao, Y., Zhang, H., Wang, P., & Zhao, X. (2015). Video Steganalysis Based on Intra Prediction Mode Calibration. *International Workshop on Digital Watermarking Springer*, *9569*, 119-133.

Xiushi Cao received the B.S. degree from the Hangzhou Dianzi University of China, Hangzhou, China, in 2017. He is currently pursuing the Master degree with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai. His research interests include video steganography.

Tanfeng Sun received the Ph.D. degree in information and communication system from Jilin University, Changchun, China, in 2003. He was a Visiting Scholar with the New Jersey Institute of Technology, Newark, NJ, USA, from 2012 to 2013. He is currently an Assistance Professor with the School of Information Security Engineering at Shanghai Jiao Tong University, Shanghai, China. His research interests include digital forensics on video forgery, digital image and video watermarking, and video's content recognition and understanding. Dr. Sun is an IEEE member.

Yi Dong received the B.S. degree with the School of Electronic Information and Electrical Engineering from Shanghai Jiao Tong University, Shanghai, China, in 2015. He is currently pursuing the Ph.D. degree with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. His research interest includes steganography and steganalysis.

Ke Xu is a post doctor of Shanghai Jiao Tong University now. They are interested in action recognition, gait recognition and abnormal event detection.