ADAPTIVE CRYPTO-STEGANOSYSTEM FOR VIDEOS BASED ON INFORMATION CONTENT AND VISUAL PERCEPTION

Prerana Mukherjee*, Siddharth Srivastava*, Brejesh Lall*, Saisha Asolkar, Meera Pai****
*** Indian Institute of Technology, Delhi. ** National Institute of Technology, Goa**

at Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG)
IIT Patna, 16th-19th December 2015

Abstract

Steganography is the art of hiding secret data inside a carrier media. Most steganographic techniques suffer from the drawback that they are unable to retain the perceptual quality. Using saliency cues for developing an adaptive steganographic technique can help to alleviate this problem. In this work, a novel perception driven robust crypto-steganographic algorithm is proposed for embedding secure data in videos. The proposed scheme selects the payload regions based on natural scene statistics. To further strengthen the scheme and ensure intractability of secure data, the encrypted secret data is embedded in a random manner using jumbling sequence generator in the frames. We utilize perceptual hashing to evaluate the number of bit insertions that will not compromise the perceptual quality. A comprehensive performance evaluation of the proposed scheme is provided to detail the effectiveness. We demonstrate that the scheme shows a lot of promise in being robust against statistical and saliency based attacks.

Methodology

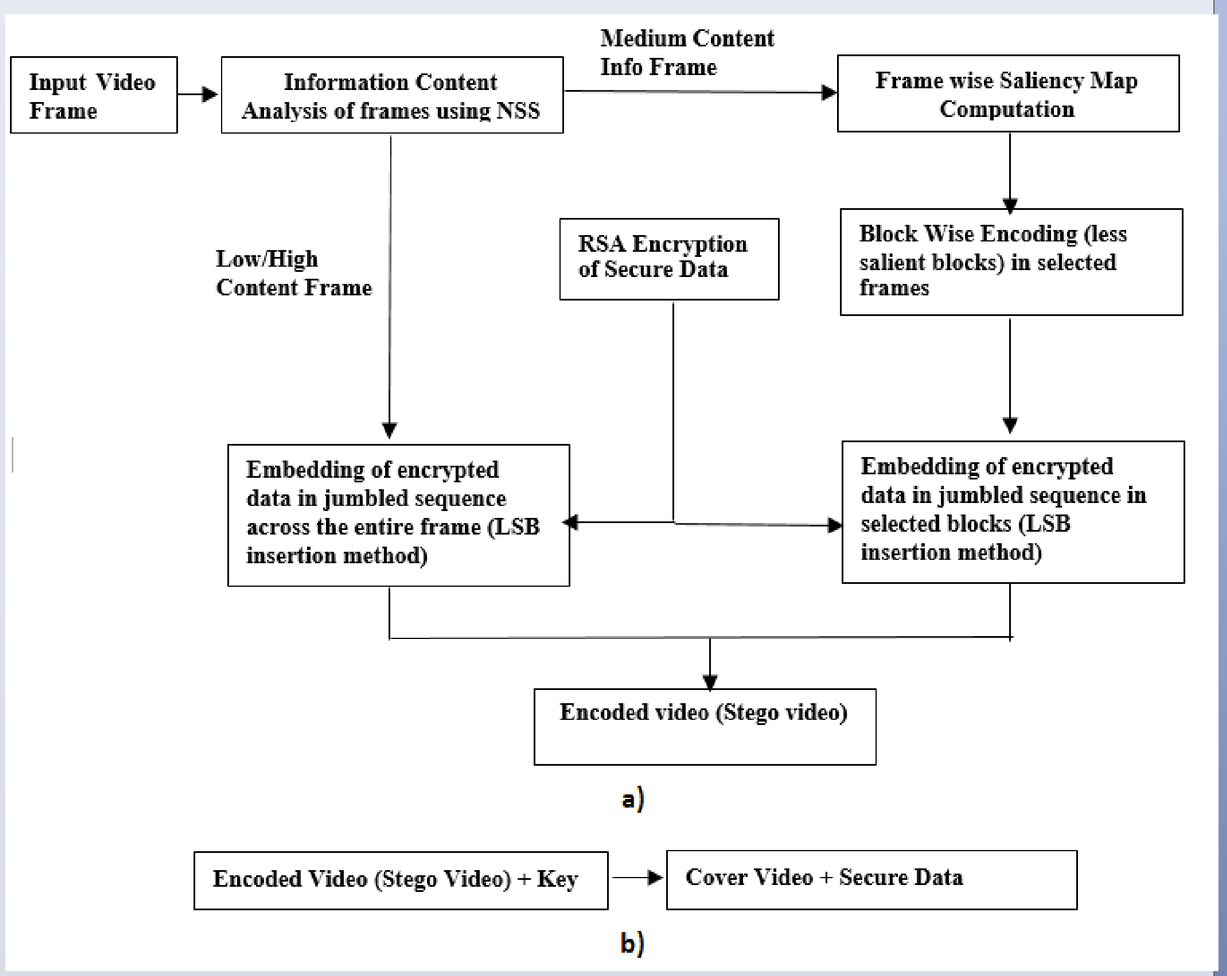

Fig. 1. Proposed Methodology: a) Encoding scheme b) Decoding Scheme

Results

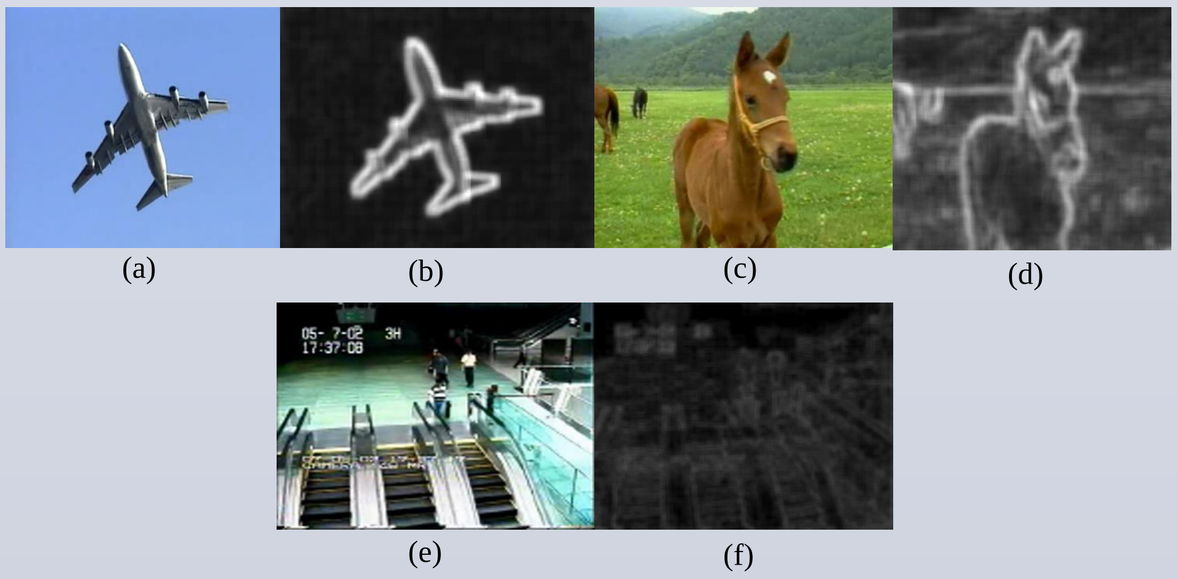

Fig. 2. Information Content Assessment using Natural Scene Statistics. 2a, 2c, 2e: Frame with low (0.1-0.3), medium (0.4-0.7) and high information content (0.8-1.0) respectively. 2b, 2d, 2f: The corresponding saliency maps for these using NSS.

Technique	MSE	PSNR	Chi-Square similarity
SEQUENTIAL	0.0119	67.3635	0.0071
BLOCK-WISE	0.00004	91.8219	2.8380e-05

Table 1. Performance Degradation

Info Content	MSE	PSNR	CWSSIM	PH	FSIMc
LOW	0.0498	63.0981	0.9993	0.381944	0.9735
MEDIUM	0.00004	91.8219	0.9998	0.027778	0.9939
HIGH	0.00023	84	1.0000	0.022569	0.9992

Table 2. Performance measures on original vs encoded stego frame.

JSteg	StegHide	OpenPuff	F5	Our Method
80.5 ± 4.2	51 ± 6.4	65.2 ± 1.6	78.5 ± 3.1	49 ± 7.8

Table 3. SVM Classification Performance using DCT features.

Fig. 3. a) Original Frame (medium content), b) Motion Map, c) Frequency Tuned Map, d) Saliency Map, e) Encoded Frame containing secure data

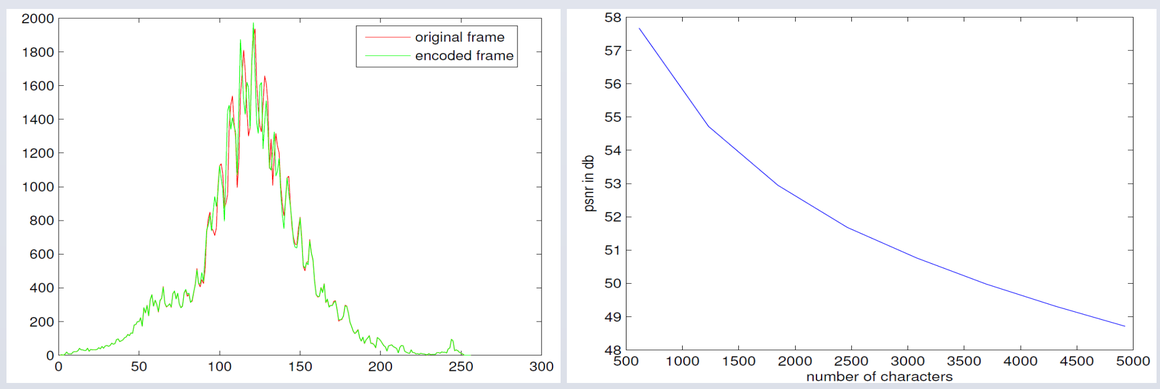

Fig. 4. a) Histograms for original and encoded (medium content) frame, b) PSNR vs number of characters encoded block-wise (medium info)

Conclusion

- The data is distributed according to the level of information content in the frames such that the change after embedding is not perceptible.
- To further strengthen the scheme, the encrypted text (using RSA) is randomly spread in the blocks.
- Steganalysis was not able to detect the presence of hidden messages in many stego frames of the encoded video and recognized them as plain cover frames, showing that the proposed scheme is robust against the statistical and saliency based steganalysis techniques.

References

- R. K. Singh and B. Lall, “Saliency map based image steganography,” in Image and Vision Computing New Zealand (IVCNZ), 2013 28th International Conference of. IEEE, 2013, pp. 430–435.
- R. Achanta, S. Hemami, F. Estrada, and S. Susstrunk, “Frequency-tuned salient region detection,” *In CVPR*, pp. 1597–1604, 2009.

Contact: Dr. Brejesh Lall (brejesh@ee.iitd.ac.in)