ISSN 2278-9723
DOI:10.31838/ijccts/09.01.03

Research Article

Curve-Let Transform Based 'Text-In-Image Steganography ' By Using Huffman Coding

LINGAMALLU NAGA SRINIVASU[1]*, VIJAYARAGHAVAN VEERAMANI[2]
[1,2]Department of Electronics and Communication Engineering, Vignan's Foundation for Science, Technology and Research, Vadlamudi, Guntur, Andhra Pradesh-522213, India
Email: lingamallusrinivas@gmail.com[1], vijayaraghavan123@gmail.com[2]
Received: 11.07.21, Revised: 12.08.21, Accepted: 11.09.21

ABSTRACT
The idea of text-in-image steganography is to embed the confidential text data into an image and to produce a high quality of stego image. Nowadays the stego image generated from text-in-image steganography process has been used majorly in surveillance and remote sensing applications. It plays a crucial role in improving security and remote sensing applications. This paper is introducing a text-in-image steganography framework. In this algorithm, a unique hiding rule is constructed by using huffman codng, curve-let transform and RPE techniques. The huffman coding technique helps to generate the "ciphertext" from the confidential data. The curve-let transform is used to generate the "detailed" and "approximation" coefficients. The hiding of confidential data in "detail" coefficient is done with using RPE technique. Stego image reconstruction is done with using inverse curve-let transform. The proposed framework has produced superior results in terms of metric values, visual quality and payload capacity.

Keywords: Huffman coding, Steganography, Curve-let coefficients, cryptography, Stego image.

1. Introduction

These days, the interpersonal sharing of data is becoming easily because of the utilization of cell phones and web [5]. In this case, the safe transfer of personal information from one person to another is a major challenge [5][6]. The security of information transfer is mainly compromised by intruders. In such circumstances, information concealing methods are exceptionally useful to keep the data secured from hackers. Three principal plausible procedures are accessible for information concealing which are cryptography, watermarking and steganography.

Watermarking conceals ownership information in source data [1]. It is fundamentally used to secure ownership data. Cryptography changes the readable data into "ciphertext" [5]. In any case, previously mentioned methods don't give total invulnerability from information breaches [7]. Steganography conceal the secret data which might be text, video, audio or image into cover medium. The cover medium may be text, video, audio or image [2][3]. The mix of cryptography and steganography methods gives a preferred security over the individual strategies [9].

In steganography, stego image can be produced by utilizing a few methods like Spread spectrum technique, Spatial domain techniques, Transform domain technique, Statistical technique, Masking and Filtering technique, Distortion technique, and so on, [8][1]. The secret information is directly incorporated into the cover object without any adjustments in the spatial domain approach. It is further characterized into Random Pixel Embedding technique (RPE) and Least Significant Bit (LSB) [2].

Increased payload capacity is a benefit of the spatial domain approach. The level of security, on the other hand, is moderate.

Information is embedded in a noise sequence via the spread spectrum approach, resulting in scrambled data. The scrambled data is embedded in the cover image to create the stego image [5]. This makes it harder to recover secret information at the receiver. The stego object is created using the transform domain technique, which involves hiding the secret data in sub-bands of the cover object [4].This improves security at the expense of payload capacity.

In order to obtain the stego object, the distortion technique alters the cover object based on the hidden data. As a result, the output contains a significant quantity of noise [1]. The secret information is hidden in prominent areas of the cover media using the masking and filtering approach. The target object is plainly visible in this case, hence it is only utilised for copy right purposes [3].

2. Proposed Method

Block diagram of introduced algorithm has been shown in Figure. 1. First the confidential data is converted into "ciphertext" by huffman coding. Later the cover image is resized into 256 × 256. In order to produce stego image, the steganography operation is performed on cover image and "ciphertext" by using curve-let transform and RPE technique.

2.1 Huffman Coding

The hufman coding helps to generate the "ciphertext" from the readable data. The word "WELCOME" is treated as a confidential data. The generation procedure of "ciphertext" from the readable data is described as follows.

Step 1: The letters of the confidential data are taken as symbols. Hence, the symbols of the considering word are "WELCOM". In a given word, the letter 'E' is repeated in two times. So, we didn't consider the second time repeated letters.

Step 2: Next, we need to find the count of each letter in the confidential data. This count is utilized to find the probabilities of symbols. The count of each letter in a given word is as follows.

W	E	L	C	O	M
1	2	1	1	1	1

Step 3: The probabilities of the symbols are calculated by using the output of step 2. It can be achieved by using the following formula.

Probability of each symbol = Count value of each symbol / Total characters of confidential data. The probabilities of a step 2 output are as follows.

W	E	L	C	O	M
0.1429	0.2857	0.1429	0.1429	0.1429	0.1429

Step 4: The dictionary values of the symbols are calculated based on probabilities by using the algorithm of maximum variance. The dictionary value of each symbol is represented as follows.

W	E	L	C	O	M
011	00	010	101	100	11

Step 5: In order to generate the "ciphertext", first we need to assign the correspondent dictionary value on each character of the confidential data. Later, all dictionary values of confidential data are concatenated to produce long length binary data. Finally, the long length binary data is split into 8 bit binary code-words. The integer forms of binary code-words are act as a "ciphertext".

The step 5 output of given word is as follows.

W	E	L	C		O	M	E
011	00	010	101		100	11	00
01100010		10110011		00**00000**			

98 179 0

2.2 Steganography Operation

This operation is used to generate the stego image by using the curve-let transform and RPE technique. First, the curve-let transform is applied on resized cover image to generate the "detailed" and "approximation" coefficients. The detailed coefficients contain insignificant information of the cover image. The "approximation" coefficients contain the significant information of the cover image. Here we need to select the "detail" coefficients to conceal the confidential data. Because, the human eyes are cannot detect abnormal changes in detail coefficients. The "ciphertext obtained from the section 2.1 is concealed in "detail" coefficients of the cover image by using RPE technique. The inverse curve-let transform is applied on "approximation" and embedded "detail" coefficients to produce stego image.

3. Results And Discussions

The results of the proposed method are discussed in this section. The confidential data is generated by the random generator. The cover images are downloaded from the "public domain" database. Initially, the "ciphertext" is generated by the confidential data using huffman coding. Next, we consider the"cameraman" cover image is shown in figure 2. Now, we apply the curve-let transform on cover image. The "approximation" and "detail" coefficients of "cameraman" cover image is shown in figure 3. Finally, the "ciphertext" is concealed in "detail" coefficients of the cover image. In order to produce stego image, the inverse curve-let transform is applied on "approximation" and embedded "detail" coefficients. The resultant image is shown in figure 4.

Fig.2: Cameraman Cover image

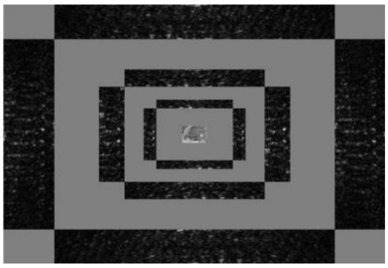

Fig.3: Curve-let Coefficients

Fig.4: Stego image

This algorithm is also tested with different cover images are shown in figure 5. The resultant images of this algorithm are shown in figure 6.

(a) Lena (b)Pout (c) Barbara (d) Baboon

Fig. 5. The cover images.

(a) Lena (b)Pout (c) Barbara (d) Baboon

Fig. 6. The stego images.

4. Metric Values of Proposed Method

In this paper, quality metrics are used to judge the quality of the proposed method. The "correlation (CORR)", "peak signal to noise ratio (PSNR)" and "number of pixels change in rate (NPCR)" are the metrics used to evaluate the quality of proposed method. The proposed method metrics compared with several methods likes "HED" [3], "WPT-NS" [2], "DE-DWT" [4], "MWLE-IWT" [1].

Table 1: PSNR metric values for various steganography methods

Cover Image	HED PSNR (dB)	WPT-NS PSNR (dB)	DE-DWT PSNR (dB)	MDLE-IWT PSNR (dB)	**Proposed Method PSNR (dB)**
Cameraman	47.444	39.021	42.894	47.254	**53.51**
Lena	47.448	38.773	42.792	47.354	**53.25**
Pout	47.812	38.456	42.783	47.567	**52.81**
Barbara	46.974	38.159	42.663	46.958	**53.92**
Baboon	47.433	39.159	42.835	47.324	**52.76**

Table 2: CORR metric values for various steganography methods

Cover Image	HED CORR	WPT-NS CORR	DE-DWT CORR	MDLE-IWT CORR	**Proposed Method CORR**
Cameraman	0.963	0.914	0.952	0.992	**0.998**
Lena	0.957	0.936	0.961	0.991	**0.999**
Pout	0.941	0.924	0.944	0.994	**0.998**
Barbara	0.977	0.919	0.961	0.991	**0.998**
Baboon	0.945	0.988	0.944	0.994	**0.997**

Table 3: NPCR metric values for various steganography methods

Cover Image	HED NPCR	WPT-NS NPCR	DE-DWT [19] NPCR	MDLE-IWT [12] NPCR	**Proposed Method NPCR**
Cameraman	0.274	0.527	0.345	0.026	**0.011**
Lena	0.232	0.477	0.365	0.026	**0.019**
Pout	0.258	0.551	0.371	0.107	**0.024**
Barbara	0.222	0.542	0.322	0.114	**0.022**
Baboon	0.207	0.507	0.348	0.107	**0.011**

Tables 1-3 compare the steganography metrics values for the "cameraman image," "lena image," "baboon image," and "barbara image." Tables 1-3 clearly illustrate that the suggested method has significantly higher metric values than previous methods. When compared to similar current methodologies, these findings clearly show that the suggested framework stego image has achieved good visual quality, higher payload capacity, and sufficient metric values.

5. Conclusion

Curve-let transform based 'text-in-image steganography ' framework using huffman coding has been proposed in this paper for producing high quality stego image. Huffman coding has been used in this algorithm for generating the "ciphertext". An efficient multi-scale direction transform which is known as curve-let transform has been applied on resized cover images in order to produce "approximation" and "detailed" coefficients.
The hiding of confidential data in "detail" coefficient is done with using RPE technique. Stego image reconstruction is done with using inverse curve-let transform. The proposed framework has produced superior results in terms of metric values, visual quality and payload capacity.

References

1. Hua Zhang, Liting Hu, "A data hiding scheme based on multidirectional line encoding and integer wavelet transform", Signal Processing: Image Communication, 2019, Vol. 78, Issue. 3, pp.331 - 344. https://doi.org/10.1016/j.image.2019.07.019
2. Randa Atta, Mohammad Ghanbari, A High Payload Steganography Mechanism Based on Wavelet Packet Transformation and Neutrosophic Set, Journal of visual communication and image representation, March 2018, Vol. 3, Issue 9, Pp: 1-28. https://doi.org/10.1016/j.jvcir.2018.03.009.
3. Shabir.A. Parah, J.A. Sheikh, J.A. Akhoon, N.A. Loan, G.M. Bhat, "Information hiding in edges: a high capacity information hiding technique using hybrid edge detection", Multimed. Tools

Appl,,.2018, Vol. 77, Issue 1, Pp: 185–207. https://doi.org/10.1007/s11042-016-4253-x ISSN 1380-7501

4. S. Atawneh, A. Almomani, H.B. Al, P. Sumari, B. Gupta, "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain", Multimedia Tools Appl., 2017, Vol. 76, Issue 18, Pp: 18451–18472. DOI 10.1007/s11042-016-3930-0
5. Shuaijianni Xu & Liang Feng Zhang, "Cryptanalysis of Morillo-Obrador polynomial delegation schemes", IET Information Security, Volume 12, Issue 2, March 2018, Pp. 127 – 132 https://doi.org/10.1049/iet-ifs.2017.0259
6. Wenying Zhang & Vincent Rijmen, "Division cryptanalysis of block ciphers with a binary diffusion layer ", IET Information Security, Volume 13, Issue 2, March 2019, Pp. 87 – 95 https://doi.org/10.1049/iet-ifs.2018.5151
7. Kumar, C., Singh, A.K. & Kumar, P. "A recent survey on image watermarking techniques and its application in e-governance", Multimedia Tools and Applications, 2018, Vol. 77, Pp: 3597–3622. https://doi.org/10.1007/s11042-017-5222-8
8. Y.Eliza Sruthi, A.Rajaiah, M.Govindu, " FPGA Implementation of Lifting DWT Based LSB Steganography", International Journal of Engineering Science and Computing, 2014, Pp: 878-884, DOI:10.4010/2014.260
9. R. De Prisco and A. De Santis, "On the Relation of Random Grid and Deterministic Visual Cryptography", in IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 653- 665, April 2014. DOI: 10.1109/TIFS.2014.2305574
10. Veeramani Vijayaraghavan, Marappan Karthikeyan, “Denoising of images using principal component analysis and undecimated dual tree complex wavelet transform”, International Journal of Biomedical Engineering and Technology, Vol. 26, Issue 3-4, Pp: 304-315. https://doi.org/10.1504/IJBET.2018.089962
11. Mohan Laavanya, Veeramani Vijayaraghavan, “Residual learning of transfer-learned AlexNet for image denoising”, IEIE Transactions on Smart Processing & Computing, Vol 2, Issue 2, Pp: 135-141 DOI: 10.5573/IEIESPC.2020.9.2.135
12. M Laavanya, V Vijayaraghavan, “Real Time Fake Currency Note Detection using Deep Learning”, 3rd National Conference on VLSI, Signal Processing & Communications, Publication date 2019/9
13. Vijayaragahvan Veeramani, Laavanya Mohan, “A Comparative Study Of Various Wavelet Approaches Used In Image Denoising”, Information Technology In Industry, Vol. 9(1), Pp: 1061- 1078. https://doi.org/10.17762/itii.v9i1.238
14. Laavanya Mohan, Vijayaragahvan Veeramani, “Image Denoising: A Comparative Study Of Various Wavelet Approaches”, Information Technology In Industry, Vol. 9(1), Pp: 1045-1060. https://doi.org/10.17762/itii.v9i1.237
15. Laavanya Mohan, Marappan Karthikeyan, “Dual tree complex wavelet transform incorporating SVD and bilateral filter for image denoising”, International Journal of Biomedical Engineering and Technology, Vol. 26, Issue 3-4, Pp: 266-278. https://doi.org/10.1504/IJBET.2018.089956