High Capacity Image Steganography using Pixel Value Differencing Method with Data Compression using Neural Network

Jayeeta Majumder, Chittaranjan Pradhan

Abstract: ***The Digital Market Is Rapidly Growing Day By Day. So, Data Hiding Is Going To Increase Its Importance. Information Can Be Hidden In Different Embedding Mediums, Known As Carriers By Using Steganography Techniques. The Carriers Are Different Multimedia Medium Such As Images, Audio Files, Video Files, And Text Files .There Are Several Techniques Present To Achieve Data Hiding Like Least Significant Bit Insertion Method And Transform Domain Technique. The Data Hidden Capacity Inside The Cover Image Totally Depends On The Properties Of The Image Like Number Of Noisy Pixels. Data Compression Provides To Hide Large Amount Of Secret Data To Increase The Capacity And The Image Steganography Based On Any Neural Network Provides That The Size And Quality Of The Stego-Image Remains Unaltered After Data Embedding. In This Paper We Propose A New Method Combined With Data Compression Along With Data Embedding Technique And After Embedding To Maintain The Quality The Communication Channel Use The Neural Network. The Compression Technique Increase The Data Hiding Capacity And The Use Of Neural Network Maintain The Flow Of Data Processing Signal***

Keywords: ***Image steganography, Data Compression, Arithmetic coding, Pixel value differencing, Neural Network***

I. INTRODUCTION

Communication using Internet is increasing rapidly in modern days. To secure our confidential data during data transmission through a public channel is a major issue in all aspect. The confidential data needs security from an unauthorized access. In digital communication secure data transfer session is very much essential. The performance of network is the major issue for secure data transmission. To maintain confidentiality and integrity of data is required for data transmission. Cryptography gives us some popular techniques [1] to protect the data from eavesdroppers and also secured communication over the channel. Steganography techniques [2] also protect the data along with no alteration.

Revised Manuscript Received on October 05, 2019.

Jayeeta Majumder, Computer Science & Engineering, Haldia Institute of Technology, Haldia, West Bengal, Email: jem2003_kolkata@yahoo.co.in

Chittaranjan Pradhan, Computer Science & Engineering, KIIT University, Bhubaneswar, Odissa,

In Steganography, the cover image is any one of the multimedia data like image, audio, video where the original secret message are embedded. After embedding of data into the cover media is known as the stego data. The human eye cannot distinguish the original cover data with stego data. In steganographic technique the unauthorized receiver cannot identify the secret data which are being transferred through the public channel. Various application like military communication, Internet of Things and multimedia [3-5] where steganography based security system is applied. In literature survey we find several numbers of combined cryptography and steganography schemes [5-6]. In the field of information security, both cryptography and steganography techniques are used. In general, image data taken as the cover media in different application.

II. RELATED WORK

Through literature survey, we found a number of image based steganographic schemes. The LSB (east Significant Bit) is the widely used methods for high data hiding capacity. The basic LSB method only consider three LSB bits replacements. In this method, after replacement the stego- image is visually good and also increase embedding capacity. By using optimal pixel adjustment process the visual quality can be improved.

In Yang [5] scheme, cover pixel are not directly modified. The secret message bits are toggled and the new toggled patterns are recorded for extracting the secret message.

Later Chen [7] proposed a modified scheme, where modulus function is used with LSB substitution which improves the visual quality for the stego-image. To minimize the distortion in the stego-image the repetition of the secret message is considered.

Then, Xu, et al. [6] proposed a steganographic scheme with fixed payload. Some researchers [7-9] designed edge-based steganographic schemes.

In paper [10], the authors classified the pixels into two categories, Edge-pixels and non-edge pixels and apply Data embedding concept.

Islam et.al [11] proposes a method which increase the high visual quality of the stego-image. The process enhances the security level.

Wu & Tsai [12] introduces Pixel Value Differencing [PVD] method.

Khodei & Faez [13] design a combination of LSB & PVD Method. It improve the embedding Capacity.

In literature survey several different PVD methods are found. A tri-way PVD approach with steganalysis method are discussed by Lee et al. [3].

Tseng &Leng [14] uses perfect square number [PSN] which improve the traditional PVD technique. Here, secret message merge with the PSN.

Liao et. al.[15] develop four pixel differencing method.

Swain [16] introduces 2X2 pixel non-overlapping PVD techniques.

In paper [17], where 3X3 non-overlapping block images are considered.

To improve payload capacity a seven-directional PVD scheme [18] are considered..

Using modulus function Zhao et. al. [19] proposed new PVD techniques

In paper [20], in adaptive approach falling-off boundary discussed.

In paper [21], the secret data bits are embedded in sequential order into another image pixel.

In this paper [22], the LSB technique is used where the reference of the colour plane are used to hide the secret bits.

In this paper we discuss a steganographic method by combining the lossless data compression with the data embedding technique to achieve higher embedding capacity with better visual quality. Without compromising image quality the proposed method enhance the embedding capacity.

III.PROPOSED ALGORITHM

Step1. The sender first take an image as its cover image and take the large amount of secret message.

Step2. Data Compression

Arithmetic coding is a lossless data compression technique. In arithmetic encoding, when a string is converted to its corresponding bits, first calculate what frequent used character are, and what are not. Then the frequently used characters stored with smaller amount of bits and non-frequent occurring characters will be stored with higher number of bits, As a result, fewer bits used in total. After data compression, output would be a stream of bits of the secret message. This bit stream is taken as the input for data embedding.

Step 3. Data Hiding

The most important part steganography is data hiding. It mainly hide the secret data into cover image. Here, we use pixel value differencing method to hide the bit stream. To calculate the difference the neighbouring pixel the data hiding capacity is determined.

Step 4. Use of Neural Network

In image processing, handling of gray scale image is the simpler one because here, each pixels have only one value. So, in network each pixel taken as one input. If, the image size is 16X16, then the total number of input neuron would be 16 *16 =256. The value of the first pixel at (0,0) will be the first neuron, the value of the second pixel at (0,1) and so on. The total image value will converted into one input vector and finally, the vector feed to the network.

In this way, after embedding the hidden data into the original image will sent to the receiver side in a secure manner.

Step 5. After accepting the stego image in the receiver side as an input and apply the reverse technique to separate the hiding message from the original cover image. The final secret message is in compressed form.

Step 6. Decompression

The secret message is now passes through the decompression technique to retrieve the original secret message.

IV. FLOWCHART OF PROPOSED ALGORITHM

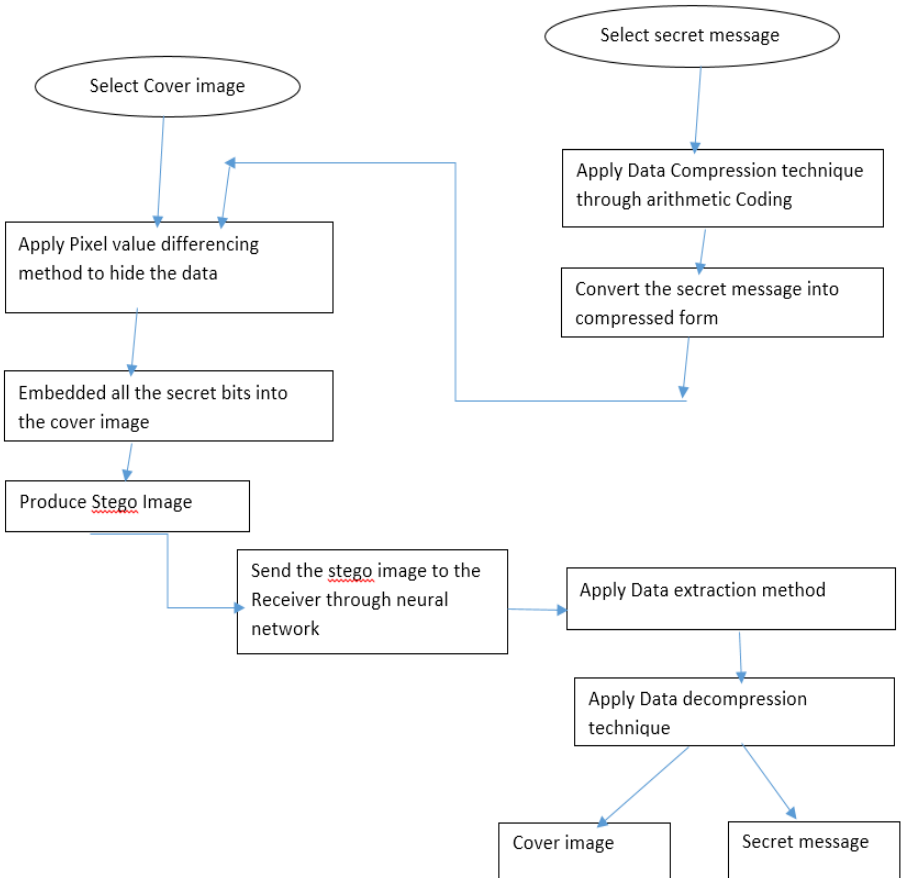


Fig 1. The flowchart of the proposed algorithm

V. EXPERIMENTAL RESULT

The stego image quality compare to the orginal cover image is measured by the parameter PSNR (Peak Signal Noise Ratio). Which is expressed in terms of dB. Here, we take few number of cover image along with a secret data to check the PSNR values. The following table shows the testing results.

a) After data Compression

Secret message

good morning all of you.

After compression

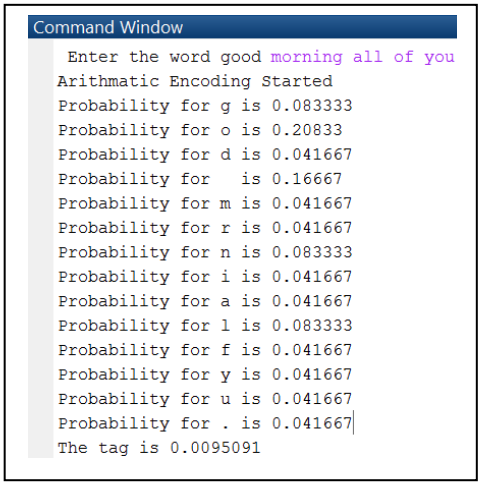
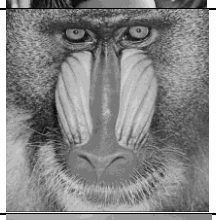
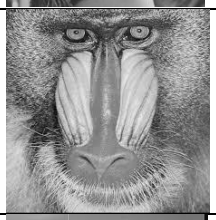
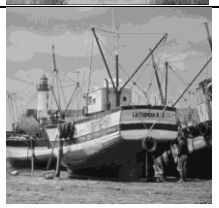


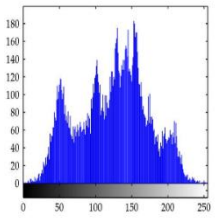
Fig 2. After Data Compression using Arithmetic Encoding

b) After Data embedding

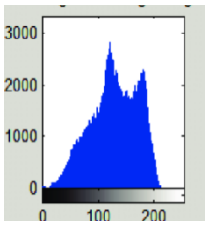
Table 1. The PSNR and MSE value of the proposed algorithm

Image name	Size	Cover Image	Stego Image	PSNR(dB)	MSE
Lena	512X512			44.5273	3.532
Baboon	512X512			38.1284	6.458
Boat	512X512			41.2546	7.254

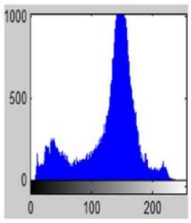
c) Histogram Analysis



a) Lena



b) Baboon



c) Boat

Fig 3. The histogram Analysis of the above stego- image

VI CONCLUSIONS

In this paper we propose a good approach of image steganography technique in the combination of Data Compression and PVD method with the help of neural network. Here, fixed image size are considered and secret information of fixed size are also considered. The neural approach uses to embed information satisfies a secure steganography. Neural Steganography is a powerful tool that enables people to communicate without possible eavesdroppers even knowing there is a form of communication.

The framework provides an effective way to select output image to accommodate the secret information. The receiver needs reverse technique of PVD along with arithmetic decoding which will be used to decode the secret message.

REFERENCES

1. LeeYP, LeeJ-C, ChenW-K, ChangK-C, SuI-J,Chang C-P.2012High-payload image hiding with quality recovery using tri-way pixel-value differencing. Inf.Sci.191, 214–225. (doi:10.1016/j.ins.2012.01.002)
2. Al-OtaibiN, GutubA.2014 Flexible stego-system for hiding text in images of personal computers based on user security priority. In Proc. Int. Conf. on Advanced Engineering Technologies (AET-2014), Dubai, UAE, pp.250–256.
3. Rafik Braham,James O Hamblen, “The design of a neural network with a biologically motivated architecture.” ,IEEE transactions on neural network, September 1990
4. Zhou X, GongW,Fu W,Jin L.2016 An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS15th Int. Conf. on Computer and Information Science (ICIS), Okayama, Japan, pp.1–4.
5. Yang C-H.2008 Inverted pattern approach to improve image quality of information hiding by LSB substitution. Pattern Recognit. 41, 2674–2683. (doi:10.1016/j.patcog.2008.01.019)
6. K. Bailey and K. Curran, “An evaluation of image based steganography methods,” Multimedia Tools and Applications, vol. 30, no. 1, pp. 55–88, 2006.
7. Chen S-K. 2011 Amodule-basedLSBsubstitution method with lossless secret data compression. Comput.Stand.Interfaces33, 367–371.(doi:10.1016/ j.csi.2010.11.002)
8. Xu W-L,Chang C-C,ChenT-S,WangL-M.2016An improved least-significant-bit substitution method using the modulo three strategy. Displays 42, 36–42.(doi:10.106/j.displa.2016.03.002)
9. ChenWJ, ChangCC, LeTH.2010 High payload steganography mechanism using hybrid edge detector.ExpertSyst.Appl.37, 3292–3301. (doi:10.1016/j.eswa.2009.09.050)
10.. . Pal AK, Pramanik T.2013 Design of an edge detection based image steganography with high embeddingcapacity.LNICST115, 794–800. (doi: 10.1007/978-3-642-37949-9_69)

11.. IslamS, Modi MR,Gupta P.2014 Edge based steganography on colored images. In Intelligent computing theories (eds DSHuang, VBevilacqua, JC Figueroa, P Premaratne). Lecture Notes in Computer Science, vol.7995, pp.593–600.Berlin, Germany: Springer.(doi:10.1007/978-3-642-39479-9_69)
12. Wu D-C, Tsai W-H.2003 A steganographic method for images by pixel value differencing. Pattern Recognit.Lett.24, 1613–1626.(doi:10.1016/S01678655(02)00402-6)
13. Khodei M, FaezK.2012 New adaptive steganographic method using least significant bit substitution and pixel value differencing. IET Image Process10,667–686.(doi:10.1049/iet-ipr.2011. 0059)
14. Tseng H-W, LengH-S. 2013 A steganographic method based on pixel-value differencing and the perfect square number.J.Appl.Math.2013, 189706. (doi:10.1155/2013/189706)
15. Liao X, WenQ-Y, ZhangJ. 2011 A steganographic method for digital images with four-pixel differencing and modified LSB substitution. J.Vis. Commun.ImageR22, 1–8. (doi:10.1016/j.jvcir. 2010.08.007)
16. Swain G.2016 A steganographic method combining LSB substitution and PVD in a block. In Int. Conf. on Computational Modeling and Security(CMS2016), pp.39–44.
17. Hosam O,Halima NB.2016 Adaptive block-based pixel value differencing steganography. Secur. Commun.Netw.9, 5036–5505.(doi:10.1002/sec. 1676)
18. Pradhan A, Sekhar KR, Swain G.2016 Digital image steganography based on seven way pixel value differencing.IndianJ.Sci.Technol.9. (doi:10.17485/ijst/2016/v9i37/88557)
19. ZhaoW, Jie Z, XinL, QiaoyanW.2015 Data embedding based on pixel value differencing and modulus function using in determinate equation. J. ChinaUniv.PostsTelecommun.22, 95–100. (doi:10.1016/S1005-8885(15)60631-8)
20.. Mandal J K, Das D.2012 Steganography using adaptive pixel value differencing (APVD) of gray images through exclusion of overflow/underflow. In 2nd Int. Conf. on Computer Science, Engineering and Applications (CCSEA-2012), Delhi, India.
21. Al-Qahtani A, Tabakh A, Gutub A.2009 Triple-A: secure RGB image steganography based on randomization. In 7th ACS/IEEE Int.Conf. on Computer Systems and Applications(AICCSA-2009), Rabat,Morocco,pp.400–403.
22. Gutub A A.2010 Pixel indicator technique for RGB image steganography. J.Emerg. Technol. Web Intel l.(JETWI)2,56–64.(doi:10.4304/jetwi. 2.1.56-64)

AUTHORS PROFILE

Jayeeta Majumder is pursuing her Doctorate in computer science from KIIT University, Bhubaneswar got enrolled in 2016 session and hes research is going on image steganography and done MCA from IGNOU, Kolkata, India. She has been working as the Assistant Professor of Computer Science at Haldia Institute of Technology, West Bengal. She has total Academic teaching experience of more than 10 years with more than 10 publications in reputed, peer reviewed National and International Journals. Her research area includes- Image Processing, Cryptography, Data Security, Soft Computing. She has Experience as a Freelance Writer, Assembly Programmer and Android Developer. She is one of the member of CSI.

Dr. Chittaranjan Pradhan is Doctorate in computer science from KIIT University of Bhubaneswar and done M.Tech in Computer Sci. & Engineering from KIIT University, Bhubaneswar, India. He has total Academic teaching experience of more than 12 years with more than 50 publications in reputed, peer reviewed National and International Journals, books & Conferences like Taylor & Francis Springer, Elsevier Science Direct, Inderscience, Annals of Computer Science, Poland, and IEEE. His research area includes- Artificial intelligence, Image processing, Computer Vision, Data Mining, Machine Learning, Watermarking. He has been in International Conference Committee of many International conferences. He has been the reviewer for various international Journal. He has authored many books published internationally and edited several books with Wiley, IGI GLOBAL Springer, etc. He is also member of various National and International professional societies in the field of engineering & research.