JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Reversible Image Steganography Based on Interpolation and Adaptive Approach

Sumeet Kaur[1*], Savina Bansal[2], R.K. Bansal [3]

[1]Research Scholar (Computer Engineering), IKGPTU, Kapurthala, India
[2,3]MRSPTU, Bathinda, India

[*]*Corresponding Author: purbasumeet@yahoo.co.in*

DOI: https://doi.org/10.26438/ijcse/v7i5.13941398 | Available online at: www.ijcseonline.org

Accepted: 24/May/2019, Published: 31/May/2019

Abstract— Information has to face certain data security related issues like confidentiality, message integrity, authorization etc while transmitted over internet, therefore need to design appropriate mechanism and techniques that ensures secrecy of private information while it is communicated over public networks has turn out to be an urgent and desired research problem. Steganography has been widely used in historical times and the also currently used with intensive interest. The advantage of steganography over cryptography is that it doesn't raise any suspicion and the message can be exchanged over a public communication channel. It is an ongoing research area having vast number of applications in distinct fields such as defense and intelligence, medical, on-line banking, on-line transactions handling, for various financial and commercial applications, to stop music piracy etc. In this paper a modified interpolation based method is used with adaptable range table to embed in pixels of interpolated image with secret bits. Proposed method can be used for applications (like for defense, and medical purposes etc) where exact retrieval of cover object at receiver side is required, due to use of reversible embedding approach. From experimental results it is observed that proposed technique achieves higher embedding capacity, acceptable value for visual quality and robustness against statistical and visual attacks.

Keywords— Steganography, Data Security, Reversible Embedding, Interpolation.

I. INTRODUCTION

Steganography is a Greek word means 'Covered or Confidential Writing'. Steganography is the science & art that involves communicating secret data in an appropriate multimedia carrier, e.g. image, audio, and video objects etc. It is mostly used on public networks acting as carrier of digital data and its purpose is to transmit a message using a digital cover medium in such a manner that no other than sender and receiver can trace presence of confidential information [1]. Security issues have become top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security.

Main advantage of steganography over the cryptography is secure communication. It does not attract the attention of attacker, whereas focus of cryptography is to protect communication from eavesdropper but in case of steganography objective is to conceal very presence of hidden message [2]. The power of steganography can thus be augmented by combining it with cryptography. Watermarking and fingerprinting are technologies that are closely related to steganography. In watermarking all of the instances of an object are "marked" in the same way. The kind of information embedded in a digital object when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection.

Image Steganography techniques are mainly classified into two types of domains: spatial domains and frequency domains. Spatial domain techniques provide high embedding capacity but less robust in nature, on the other hand transform domain techniques have less embedding capacity but capable of tolerating various attacks like cropping, compression, scaling etc.

Image steganography is the most popular and image has much redundancy to support embedding of secret message and further can also consider advantage of our limited visual perception of colours. Hence images are the most widely used medium being used today over the internet and this field is continually growing as is power of computer graphics. For all major image file formats (BMP, GIFF, TIFF, JPEG etc) there are different methods of hiding messages, with their own pro and cons. If a technique provides high payload capacity it may be less robust and vice versa. Patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. On the other hand, Least Significant Bit (LSB) methods in both BMP and GIF provide very high payload capacity and also very simple techniques, but very sensitive to various attacks. Majority of image data hiding techniques use uncompressed formats like BMP or GIF because they have much redundancy and hence are able to accommodate higher volume of secret data. Although uncompressed formats are more convenient for data hiding algorithms, but now it is also going to be used with JPEG image because these are popular format on the internet [3]. There is need to design secure and robust steganography algorithm to carry sensitive data over public networks to resist against steganalysis attacks [4].

Further in the paper, Section II covers review of image interpolation and various interpolation methods, Section III covers about reversible embedding, Section IV describes proposed embedding system and algorithm, Section V presents experimental results and discussion. Section VI and VII cover conclusion and also direction for future research.

II. IMAGE INTERPOLATION

Image interpolation is an essential tool in digital processing of images and also bridging the continuous world and the discrete world. Image interpolation is generally used for resolution improvement, image up or down sampling, image resizing, digital magnification and zooming etc. Image interpolation methods have also occupied a special position in medical image processing specially used In Computed Tomography (CT), Magnetic Resonance Imaging (MRI), Computer Aided Diagnosis (CAD), Computer Assisted Surgery (CAS), Picture Archiving and Communication Systems (PACS) etc [5].

III. INTERPOLATION METHODS

There are a wide variety of possible interpolation methods are available. Each method has its own pros and cons. Some of the commonly used interpolation methods are Nearest Neighbour Interpolation, Bicubic Interpolation, Bilinear Interpolation, B-Spline Interpolation, Cubic Spline Interpolation etc.

A. Nearest-Neighbour Interpolation

Using this algorithm, value of nearest pixel is assigned to the pixel in the output visualization. It is the fastest interpolation method but the resulting output image may contain toothed edges.

B. Linear Interpolation

It checks for two nearby pixels, then draws a line between these and computes a value along that line as the output pixel value.

C. Bilinear Interpolation

It checks for four nearby closest pixels, computes a weighted average based on the closeness and brightness of the considered pixels and assigns that computed value to the pixel in the output image.

D. Cubic Convolution Interpolation

This algorithm is used if a higher degree of accuracy is required. However, with still images, the difference between images interpolated with bilinear and cubic convolution algorithms is generally unnoticeable.

E. Trilinear Interpolation

This algorithm checks for the eight adjacent pixels occurring along the x, y and z dimensions, finds out a weighted average based on the closeness and brightness of the considered pixels and assigns calculated value to the pixel in the output image.

F. Cubic Convolution Interpolation

This method uses cubic polynomial waveforms instead of linear waveforms when resembling a pixel. With a one-dimension source, this method checks for four nearest pixels. With a two-dimension source, the method checks for sixteen pixels. It results in very high accuracy, thus maintaining the highest amount of fine details in the output image, but cubic interpolation requires higher processing time.

Another recent application of interpolation is data embedding. Interpolation schemes can be used to embed secret message into the interpolated virtual pixels of original cover image. Interpolation finds a new pixel by analyzing the neighbouring and adjacent pixels [6],[7],[8],[9],[10],[11],[12],[13],[14]. Researchers are also working on adaptive embedding approaches to increase robustness and using compression to increase hiding capacity.

IV. REVERSIBLE DATA EMBEDDING

Reversible data embedding means that after extracting the hidden data, original digital object can be recovered back without any distortion. From application point of view, by embedding its message verification code, reversible data hiding schemes provide a true self confirmation scheme, without the use of metadata. These schemes can support to carry sensitive data for defence, intelligent services and medical images etc. There are various reversible data hiding methods based on different techniques like Interpolation based, 'Difference expansion' and 'Histogram based shifting techniques' etc [15],[16].

V. EMBEDDING ALGORITHM

Proposed embedding method is reversible embedding method that is based on modified neighbour mean interpolation. This scheme also involves use of adaptive intensity range table based on concepts of human visual perception system. Here large no of bits are embedded for pixels belonging to high intensity value and small no of bits are embedded to pixels corresponding to low intensity value. Main purpose of using adaptive intensity range table is to design more robust embedding algorithm to resist against various attacks. Following steps are used as part of embedding secret data into interpolated cover object:

(i) Secret data is encoded into gray code and XORed with key say k1.
(ii) Cover image of size 512*512 is first scaled down into size of 256* 256 then it is interpolated by inserting additional rows and columns. Values of interpolated pixels are computed using MNMI method.
(iii) Interpolated cover image is divided into 2*2 non-overlapping blocks for each block. Pixels in each block are traversed in a zigzag order and for scanned order key k2 is used.
(iv) Absolute magnitude of difference values say Md1 and Md2 are computed for pixels in the considered block like Md(i,1)=|Qi(1,1)-Qi(0,1)| an Md(i,2)=|Qi(1,1)-Qi(1,0)|, where Q(i,j) is pixel of selected block
(v) To decide about no of bits to be embedded in changeable pixels of interpolated image an adaptive range table is generated by using rule: if upper and lower range for intensity difference values of selected pixels from current traversed block are Ul (i,1) and Ll (i,1) respectively then number of secret bits to be embedded are decided by Eb(i,1)=log2(Ul(i,1)-Ll(i,1)+1) & Eb(i,2)=log2(Ul(i,2)-Ll(i,2)+1)
(vi) Absolute magnitude of new difference values are recomputed using Md(i,1)=|Ll(i,1)+S(i,1)|& |Ll(i,1)+S(i,1), where S(i,j) is corresponding to selected element of secret data.
(vii) Pixels are embedded as decided from intensity range table as new pixel values to generate stego block.
(viii) Return to steps (ii) and all steps are repeated for all the remaining blocks of cover image and finally output stego image is obtained.

VI. EXPERIMENTS AND RESULTS

In this research work focus is over gray scale images and some standard benchmark images are considered to perform various experiments. In following part of paper results from visual analysis, statistical analysis is shown to prove the strength of the technique.

A. Visual Analysis

Using proposed technique secret data is embedded in cover object to generate stego image. Stego image is visually analysed to check for quality after embedding and it was observed that visually stego image matches with cover image. Visual analysis of cover and stego images proves high quality of proposed technique.

B. Statistical analysis

Certain statistical parameters are computed for the purpose of performance analysis of proposed embedding technique and some of results are shown here. From experiment results it is clear that very satisfactory values are achieved for all considered statistical parameters that further prove feasibility of proposed work.

1) Peak Signal to Noise Ratio (PSNR)

PSNR objectively quantifies the error signal. It is very fast and easy to implement. The high PSNR value means high security of embedding method because it signifies minimum difference between the original cover and stego images. It is computed by using following equation

$$\mathrm{PSNR}=10\log_{10}\left(\frac{255^{\wedge}2}{MSE}\right) \qquad (1)$$

2) Mean Square Error (MSE)

MSE quantifies the cumulative squared error between original cover image and stego image. Lesser the MSE higher the quality of stego image generated after embedding with secret message. It is computed by using following equation

$$\mathrm{MSE} = \frac{1}{y*z}\sum_{i=0}^{y}\sum_{j=1}^{z}\big(C(i,j) - S(i,j)\big)^2 \qquad (2)$$

Table1. Experimental results for proposed method in terms of various quality metrics Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE)

Cover Image	PSNR	MSE
Baboon	31.7686	43.6132
Lena	35.2205	19.6982
Pepper	37.3774	11.9878
Boat	33.574	27.5423
Airplane	36.7323	13.9075

Table2. Comparison of Existing well known reversible steganography techniques based on different interpolation methods and proposed method

PSNR(db), Capacity(bits)				
Cover Image	Quality	Jung and	Lu et al	Proposed
Size(512*512)	Metrics	Yoo [7]	[12]	Method
Baboon	PSNR	23.13	28.39	31.7686
	Capacity	460740	185940	655368
Lena	PSNR	30.61	33.92	35.2205
	Capacity	235460	249763	655368
Pepper	PSNR	32.02	33.32	37.3774
	Capacity	202238	237854	655368
Boat	PSNR	28.62	30.37	33.5734

	Capacity	226159	227687	655368
Airplane	PSNR	30.54	33.61	36.7323
	Capacity	188939	246811	655368

From results shown in table1 and table2, it is experientially shown that proposed approach has reasonable acceptable values for quality parameters say PSNR, MSER.

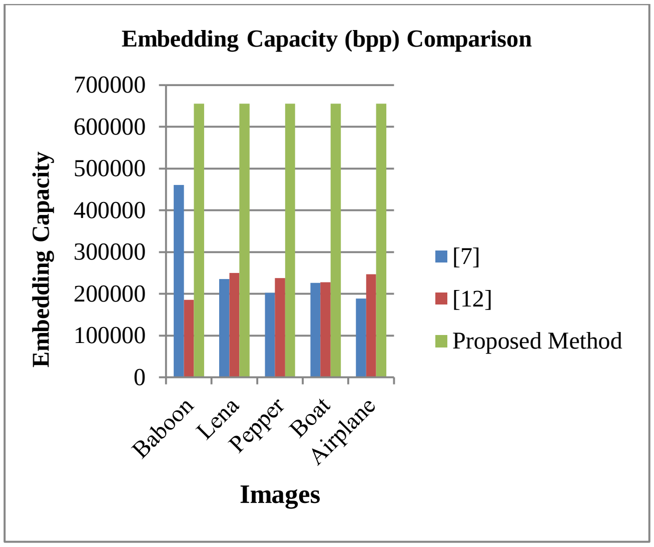

Figure 1.Comparison of proposed techniques with other techniques for Embedding Capacity parameter

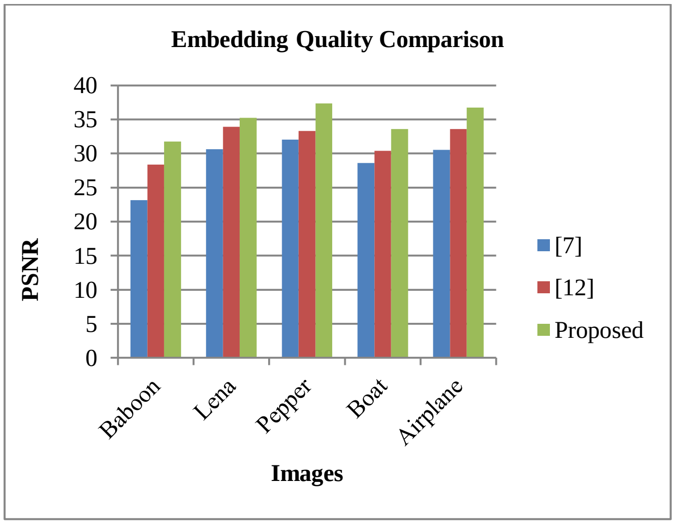

Figure 2.Comparison of proposed techniques with other techniques for Embedding quality parameter

In figure 1. and figure 2. comparative analysis of proposed technique is shown with other existing well known techniques. It is experimentally proved that proposed technique has higher PSNR and higher imperceptibility. Embedding capacity of proposed techniques is also higher as compared to existing well known techniques that further shows strength of designed technique.

VII. Future work

Future work may involve implementation of different steganalysis attacks and test to check security of the proposed technique and making it more robust. Further stronger encryption procedure can also be combined with proposed steganography approach to provide supplementary layer of security. Other future work may involve use of compression over secret data to increase embedding capacity, extending technique to different file formats, colour images etc.

VIII. Conclusion

When cryptography alone is used with digital objects, it can raise doubt about some secret information being exchanged and may provide sign to staganoanalyser to generate certain attacks and create potential threats to security of embedded secret message. The government of various countries also disagreed with individuals and businesses on the issue of public use of strong encryption products. In this paper research work for design of secure reversible steganography method is proposed. From experiment results it is evident that proposed method provides high embedding capacity, acceptable value of PSNR and MSE. From experiment results it is also observed that proposed method also resists against statistical and visual attacks that support robustness of work. Further designed technique also provides lossless recovery of cover object at receiver side.

Steganography is not a new idea, but still significant research is required in this field to develop robust algorithms that are strong enough to defend against different steganalysis attacks. There is also need to be aware of the potential benefits of this technology that can be served to society. Further research in this field will also help to generate possibilities for protection related to data integrity, dealing with other security related concerns such as confidentiality and preserving ownership etc of data while communicated over public network.

REFERENCES

[1] R. J. Anderson and F. A. P. Petitcolas, "*On the limits of steganography*," in IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 474-481, May 1998.

[2] Kodge B. G., "*Information Security: A Review on Steganography with Cryptography for Secured Data Transaction*", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.6, pp.1-4, 2017.

[3] J. Fridrich, "*Steganography in digital Media: Principles, Algorithms, and Applications*", Cambridge University Press, 2009.

[4] H. Wang & S. Wang, "*Cyber warfare: Steganography vs. Steganalysis*", Communications of the ACM, Vol. 47 No. 10, pp 76-82, 2004.

[5] T. M. Lehmann, C. Gonner and K. Spitzer, "*Survey: interpolation methods in medical image processing*," in IEEE Transactions on Medical Imaging, vol. 18, no. 11, pp. 1049-1075, Nov. 1999.

[6] Lei Zhang and Xiaolin Wu, "*An edge-guided image interpolation algorithm via directional filtering and data fusion*," in IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2226-2238, Aug. 2006.

[7] Ki-Hyun Jung, Kee-Young Yoo, "*Data hiding method using image interpolation*," Computer Standards & Interfaces, Volume 31, Issue 2, Pages 465-470, 2009.

[8] L. Luo, Z. Chen, M. Chen, X. Zeng and Z. Xiong, "*Reversible Image Watermarking Using Interpolation Technique*," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, pp. 187-193, March 2010.

[9] Wien Hong, Tung-Shou Chen "*Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism*," J ournal of Visual Communication and Image Representation, Volume 22, Issue 2, pp 131-140, 2011.

[10] Ya-Ting Chang, Cheng-Ta Huang, Chin-Feng Lee, Shiuh-Jeng Wang, "Image interpolating based data hiding in conjunction with pixel-shifting of histogram", The Journal of Supercomputing Volume 66, Number 2, pp 1093-1110. 2013.

[11] Lu, Tzu-Chuen, Chin-Chen Chang, and Ying-Hsuan Huang. "*High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting*", Multimedia Tools and Applications, volume 72, issue 1, pp 417–435, 2014.

[12] Yuan-Yu Tsai, Jian-Ting Chen, Yin-Chi Kuo, and Chi-Shiang Chan, "A generalized image interpolation-based reversible data hiding scheme with high embedding capacity and image quality", KSII Transactions on Internet and Information Systems (TIIS) VOL. 8, NO. 9, pp 3286-3301, Sep. 2014.

[13] Mingwei Tang, Shenke Zeng, Xiaoliang Chen, Jie Hu, Yajun Du, "An adaptive image steganography using AMBTC compression and interpolation technique," Optik, Volume 127, Issue 1, pp 471-477, 2016.

[14] Tzu-Chuen Lu, "An interpolation-based lossless hiding scheme based on message recoding mechanism," Optik, Volume 130, pp 1377-1396, 2017.

[15] Jun Tian, "Reversible data embedding using a difference expansion," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp 890-896, Aug. 2003.

[16] Chia-Chen Lin, Wei-Liang Tai, Chin-Chen Chang, "Multilevel reversible data hiding based on histogram modification of difference images," Pattern Recognition, Volume 41, Issue 12, pp 3582-3591, 2008.

AUTHOR'S PROFILE

Dr. Savina Bansal area of research is High Performance, Energy efficient and Fault-tolerant Computing, WSNs, Wireless Communications. She has around 30 years of teaching experience and presented more than 100 research papers in various international and national journals and conferences. She had guided 02 Ph.D.s and around 50 M.Tech. students for dissertation work.

Dr. R.K. Bansal area of research is Real-time Computing, Wireless Sensor Networks. He has more than 32 years of teaching experience and presented around 80 research papers in various international and national journals and conferences. He had guided 01 Ph.D. and around 25 M.Tech. students for dissertation work.

Sumeet Kaur is pursuing her Ph.D. from IKG-PTU, Kapurthala. Her area of research is image processing and steganography. She has around 50 publications in various international and national journals and conferences. .