



e-ISSN:2582-7219



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 4, April 2023



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.54



6381 907 438



6381 907 438



ijmrset@gmail.com



www.ijmrset.com



Data Embedding Method Using Adaptive Pixel Pair Matching Algorithm

C.Vaisnavi, Ms.Geetha

II MCA, Department of MCA, Paavai Engineering College, Paavai Nagar, Pachal, Tamilnadu, India

Professor, Department of MCA, Paavai Engineering College, Paavai Nagar, Pachal, Tamilnadu, India

ABSTRACT: Data Hiding or steganography has been an important communication network since people started communication in writing. The main aim in steganography is to hide a secret message within cover media in such a way that an observer cannot detect the presence of contents of the hidden message. Cover images/video are original images without secret data and after embedding secret data they are called as stego images. steganography and cryptography are the parts in digital security the obvious advantage of steganography over cryptography is that messages do not attract attention to themselves, to messengers, or to recipients. The progress in steganography has also led to many serious problems such as hacking, compression, reformat, etc. steganography finds its role in attempting to address these growing concerns, with the use of steganography techniques, it is possible to hide secret information within images, audio and video files which are statistically undetectable. This present work proposes a new data embedding technique which uses two pixels sequentially one after another which is known as pixel pair matching (PPM) technique. The two pixel is then replaced by the searched coordinate to store the digit. The APPM (Adaptive Pixel Pair Matching) method offers lower distortion than DE (Diamond Encoding) by providing more compact neighborhood sets and allowing embedded digits in any notational system.

I. INTRODUCTION

As need of Internet-based applications is highly increased, so it is required to use the secrecy in communication. To achieve this goal, there are mainly three techniques are available, cryptography, watermarking and steganography. Steganography is the art of embedding the information through original object in such a behavior that the continuation of the message is unknown. The term steganography is coming from Greek word Steganos, which means, "Covered Writing". The original objects can be referred to as covered/carrier objects. After inserting the secret message in to the cover image it is called as stego image. A stego key is used for hiding. Steganography is different from cryptography. The main objective of cryptography is to secure communications by using encryption techniques. But steganography techniques are used to hide the messages, which makes difficult for a third party / person to find out the message. Watermarking and fingerprinting related to steganography are basically used for academic property protection. This method is used to hide a secret message in a text message for that number of tabs, white spaces, and capital letters, just like Morse code is used. In earlier day this technique is in very much boom but after booming of Internet and different type of digital file formats its importance gets decreased. This method is used to hide a secret message in a text message for that number of tabs, white spaces, and capital letters, just like Morse code is used. In earlier day this technique is in very much boom but after booming of Internet and different type of digital file formats its importance gets decreased.

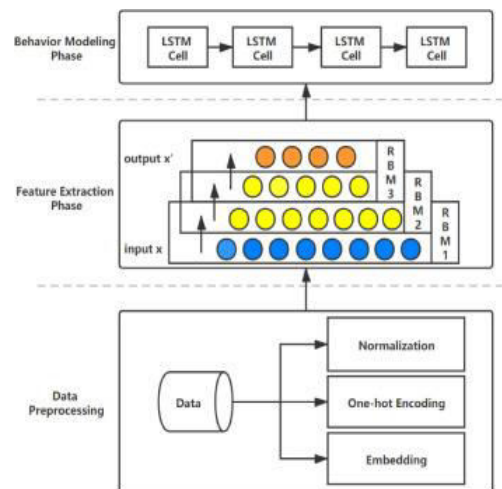


Fig 1: LSTM Based Data Embedding

Audio steganography is another type of steganography in which the properties of the human ear is considered to hide information. An audible, sound can be made inaudible in the presence of another louder audible sound. Audio steganography uses only digital audio formats such as WAVE, MIDI, AVI MPEG or etc. There are many versions present in spatial steganography that all are related to make changes directly with some bits of the digital image pixel values to hide data. Least significant bit (LSB) - based steganography is one of the simplest techniques/method that is used to hide a secret message in digital image. In this technique the pixel value of least significant bit (LSB) are get replaced with bits of secret message and all this is done without introducing many perceptible distortions. The embedding of message bits can be done either sequentially or randomly. In spatial domain following techniques comes these are as follows such as LSB substitution/replacement, LSB matching, Matrix embedding and Pixel value, differencing etc.

II. LITERATURE SURVEY

In Paper “An Image Steganographic Scheme Based on PixelValue Differencing and LSB Replacement Methods” author proposed a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be anticipated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method provides a better imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. This method hides large data with the help of LSB substitution at edge area of image and uses the PVD for smooth region of image to hide the data. Though this technique provides larger capacity but has low visual quality as well as this method is complex.

In paper “Hiding Data in Images by Simple LSB Substitution” authors proposed an LSB substitution for hiding the data into the image. To achieve better visual quality of stegoimage it takes care of noise sensitive area for embedding. This method intelligently differentiates normal texture and edges area of an image as well as it takes the advantage of these areas for the embedding. This method analyses the different LSB values as well as edges, texture masking and brightness of the cover image to calculate the number of kbit LSB for secret data embedding. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. Optimal pixel adjustment process is also used to generate the stego-image which is obtained by the simple LSB substitution method. The proposed method also termed as OPAP (Optimal Pixel Adjustment Process). The overall result shows a good high hidden capacity with high image quality of the stego-image can be greatly improved with low extra computational complexity. The main shortcoming of this technique is the worst mean-square-error between the stego-image and the cover image is derived.

In paper “Efficient Steganographic Embedding by Exploiting Modification Direction” author provides a new approach to data hiding scheme by introducing a novel method of steganographic embedding in digital images is described, in which each secret digit in a $(2n+1)$ notational system is carried and hide by n pixels of the cover image. In this method



at most only one pixel is increased or decreased by 1. It is not suitable for applications that requiring high payload is the main shortcoming of this technique.

In paper “A Novel Image Data Hiding Scheme with Diamond Encoding” author provides a new approach to data hiding scheme by introducing Diamond Encoding. In this technique, first the process is portioning and embedding of the cover image into non-overlapping blocks of two consecutive pixels. Then it transforms the secret messages into a series of digits which are equivalent to those blocks. Afterward the diamond encoding technique is applied on those blocks to calculate the diamond characteristic values i.e. DCV to hide/concealed secret B-ary digits into the diamond characteristic values. After that the diamond characteristic value is gets modified by secret message digit and which can be done by adjusting pixel values in blocks. The main shortcoming of this technique is that it suffers from higher distortion for various lower payload with lower image quality and can be attacked by capacity in terms of payload and performance that can be improved. The PPM-based method, suppose a digit TB is to be concealed. The range of TB is between 0 and B-1, and a coordinate (p', q') in $\emptyset(p, q)$ has to be found such that $f(p', q') = TB$. [2] Therefore, the range of (p, q) must be integers between 0 and B-1, and each integer must occur at least once. In addition, to reduce the distortion, the number of coordinates in $\emptyset(p, q)$ should be as small as possible. The best PPM method shall satisfy the following three requirements:

III. METHODS

Before embedding or hiding the secret message in to the cover image it is inputted to encryptor for the encryption. As well as after the extraction process again this secret message is passed to decryptor for decryption and then the original message is obtain. The advantage of this methodology is that it protects the secret message from the attacker under the steganalysis attack. In addition to English language, this secured APPM technique is also able to hide data provided in different languages such as Marathi, Hindi etc

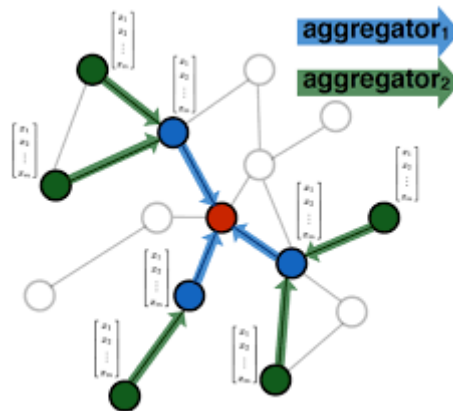


Fig 2: Aggregator

The embedding module accepts the encrypted secret message as input from encryptor module and process on it to embed that encrypted secret message in to cover image as a steganography for the secret communication. The output of this embedding module is the stego image which contains a secret message. Suppose the cover image is of size $U \times U$ and M is the message bits to be concealed. The size of is T is $|T|$ and key E_r .

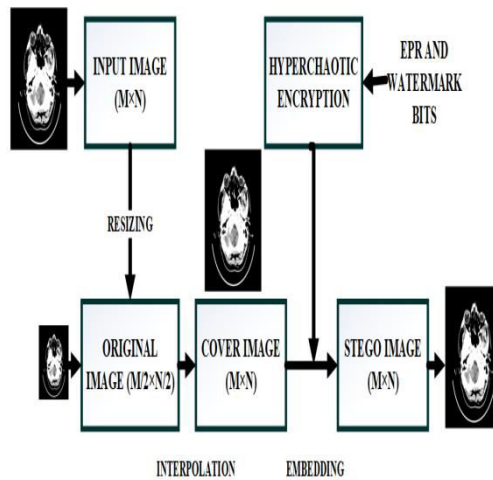


Fig 3: Work Flow

In digital watermark module a digital watermark is implemented. A digital watermark is a kind of marker which is secretly embedded in a noise-tolerant signal such as image, video, audio and text etc. Digital watermarks may be used to verify the authenticity; integrity of the carrier signal as well as it shows the identity of its creator/owner. It gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (Authentication and non repudiation) and that the message was not altered in transit (i.e. to maintain integrity). As well as watermark gives integrity of message. The digital watermark gives authentication for secured communication. In this system message received from sender is in authenticated form and with security in communication. Due to this sender cannot deny about message sent by him and this also assures that message was not altered in transit.

IV. RESULT ANALYSIS

T is a predefined threshold. A larger D indicates that Hh and Hv have larger differences and thus, the image is likely to have messages embedded. [2] The fig.8 shows the security analysis and comparison of histogram of stego and cover images. From these figures we can say that the histogram of cover and stego images are equal. To detect the presence of secret message we employ the security analysis and steganalysis attack on these images but the results produced from them shows that the Secured APPM technique is secure under the detection of some well known steganalysis techniques.

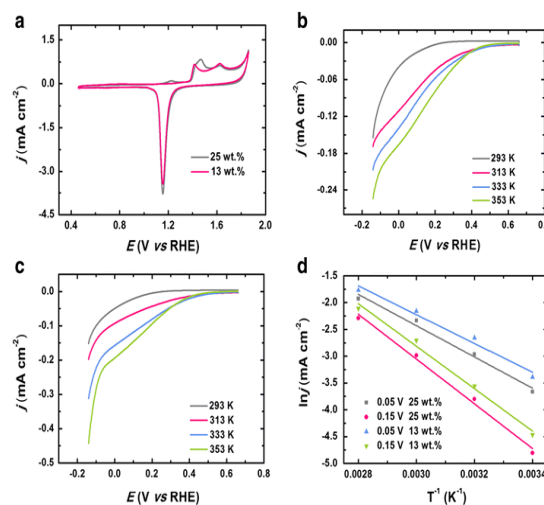


Fig 4: Result Analysis



In this section, we analyze the security of Secured APPM under statistical steganalysis schemes, including the HVDH scheme. The HVDH [15] scheme is used to detect the presence of hiding message according to the distance between vertical and horizontal histograms. [15] The proposed a detection method based on the statistical analysis of histogram differences. Zhao et al. [15] observed that for many pair wise embedding methods, the difference between the horizontal difference histograms and vertical difference histograms are significantly altered. Zhao et al. [15] use the distance between Hh and Hv as a statistical detector to detect the abnormality of histogram. [15] The distance is defined as This section shows the various types of results of Secured APPM technique with different parameters. These results show improvement over previous APPM techniques with respect to Mean Square Error (MSE). The cover and stego images which do not show any artifacts after applying Secured APPM technique to the cover image to hide the secret message in to it.

V. CONCLUSION

This paper proposed a simple and efficient data embedding method named as Secured APPM based on APPM. In that two pixels are used as an embedding unit and a specially designed compact neighborhood set is used to embed secret message digits in to a smallest possible notational system by allowing users to select digits in any notational system for the data embedding. The proposed method not only resolves the low-payload problem in EMD, but also offers smaller MSE than OPAP, DE and APPM. It also provides a better image quality because Secured APPM does not produce any artifacts in stego images. The steganalysis results of stego images are similar to those of the cover images, which offer a secure communication under adjustable embedding capacity. It also contains additional features such as digital watermark and encryption of secret messages for the provision of more security. The secured APPM technique is also able to hide all different types of data provided to it in languages like English, Marathi, and Hindi etc. As well as this technique is secure under the detection of some well-known steganalysis techniques. All these various features made a Secured APPM technique a straightforward, economical embedding method for the data hiding. In future Secured APPM may have a chance to increase the capacity of data embedding in the cover images of it. Also there may be a chance of little improvement of MSE in it and chance to provide more security.

REFERENCES

- [1] W. Zhang, X. Zhang, and S. Wang, "A double layered plusminus one data embedding scheme," *IEEE Signal Process. Lett.*, vol. 14, no. 11, pp. 848–851, Nov. 2007.
- [2] Wien Hong and Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, February 2012.
- [3] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," *EURASIP J. Inf. Security*, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.
- [4] Swapnil S. Thakare and Niranjana L. Bhale, "A Review of Digital Image Steganography Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 4, Issue 6, June 2014, pp. 465-471, ISSN: 2277 128X.
- [5] M. Lakshmi Prasanna and Sk. Mahaboob Basha, "Extended Adaptive Pixel Pair Matching", *International Journal of Engineering Research and Applications*, Vol. 3, Issue 3, May-Jun 2013, pp.1484-1490, ISSN: 2248- 9622.
- [6] Pratap Chandra Mandal, "Modern Steganographic technique: A Survey", *International Journal of Computer Science & Engineering Technology (IJCSET)* Vol. 3 No. 9 Sep 2012.
- [7] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", *International Journal of Advanced Science and Technology* Vol. 54, May, 2013
- [8] Hsien-Chu Wu Na-I Wu Chwei-Shyong Tsai MinShiang Hwang, "An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods", *National Science Council, Taiwan*, Nov 2004.
- [9] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.* vol. 10, no. 11, pp. 781–783, Nov. 2006.
- [10]K. Chan, L. M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern Recognition*, vol. 37, no: 3, pp: 469–474, 2004.
- [11]J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.* vol. 13, no. 5, pp. 285–287, May 2006.
- [12]J. Fridrich and D. Soukal, "Matrix embedding for large payloads," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 390–394, Sep. 2006.
- [13]W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," *J. Vis. Commun. Image Represent*, Vol: 22, no. 2, pp. 131– 140, 2011.



- [14]M. Tanvir Parvez and A. Abdul-Aziz Gutub, “RGB Intensity Based Variable-Bits Image Steganography”, IEEE Asia-Pacific Services Computing Conference, pp. 1322-1327. 2008.
- [15]H. Zhao, H. Wang, and M. K. Khan, “Statistical analysis of several reversible data hiding algorithms,” in Proc. Multimedia Tools and Applications, 2009, DOI: 10.1007/s11042-009-0380



INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor
7.54

ISSN

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com