Journal of American Science

Websites:
http://www.jofamericanscience.org
http://www.sciencepub.net

Emails:
editor@sciencepub.net
sciencepub@gmail.com

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

REVIEW OF LITERATURE ON STEGANOGRAPHY IMAGE METHODS RELATED TO DIFFERENTIATION OF ADAPTIVE PIXEL VALUE AND THE EXPLOITATIONOF SEVERAL DIRECTIONS

* Prasad HM and ** Dr. Kamal Srivastava

[1]Research Scholar, Department of Computer Science, SunRise University, Alwar, Rajasthan (India)
[2]Associate Professor, Department of Computer Science, SunRise University, Alwar, Rajasthan (India)
Email: parsadworld8@gmail.com

Abstract: Steganography is the art of concealing information in a cover media in such a way that the presence of the information is unknown. Digital image steganography accomplishes the potential for protected communication that is crucial in most of the applications nowadays. Steganography has several beneficial applications. It has been driven to the frontrunner of present security systems by the amazing development in computational power, the rise in security consciousness. The main challenge in proposing a steganographic technique is to maintain a suitable balance among higher embedding capacity, imperceptibility, and security that separate it from correlated systems like cryptography and watermarking. This article offers an extensive state-of-the-art review and analysis of some recent steganographic techniques. Furthermore, we have discussed popular steganography tools in detail. Challenges in the recent deep learning based steganographic techniques have been addressed. To explore the domain, the article concludes with mentioning some future research directions.

[HM, Prasad and Srivastava, K. **REVIEW OF LITERATURE ON STEGANOGRAPHY IMAGE METHODS RELATED TO DIFFERENTIATION OF ADAPTIVE PIXEL VALUE AND THE EXPLOITATION OF SEVERAL DIRECTIONS.** *J Am Sci* 2024;20(3):25-28]. ISSN 1545-1003 (print); ISSN 2375-7264 (online). http://www.jofamericanscience.org. 05. doi:10.7537/marsjas200324.05.

Keywords: REVIEW OF LITERATURE, STEGANOGRAPHY, ADAPTIVE PIXEL

Introduction:

The internet revolution offers ease in digital communication; at the same time, it is also a challenge for us to secure the message over the open network. The security system plays a vital role to restrict the messages from being seized by an unauthorized person. Cryptography [1] protects the content of the information that allows only the sender and intended beneficiary of communication to view its contents. Information hiding techniques include steganography [2], [3] and watermarking [4]. Both watermarking and steganography are used to obscure the confidential information within the innocent media like image, video, audio, and text, but both have different purposes. Watermarking is used for authentication and copyright protection of digital data. In contrast, steganography [5] is the art of concealing information. Imperceptibility is of major importance for steganographic technique, whereas watermarking provides the maximum importance to robustness. On the basis of the capability of recovering the cover images, data hiding techniques are categorized into two groups: irreversible [6] and reversible data hiding (RDH) [7]. If the cover image can be obtained after removal of the confidential data the process is said to be reversible data hiding; otherwise it is termed as irreversible data hiding. DE, histogram shifting, and Interpolation based techniques, etc., are the examples of reversible data hiding techniques whereas LSB, PVD, etc., are examples of irreversible data hiding techniques.

Conversely, steganalysis [8], is the art of identifying the hidden information embedded in digital media. After the heart-breaking incidents of 11th September 2001, researchers have given great importance to the topic steganography and steganalysis [3]. It has also now become an important research topic due to the popularity of social media applications like Facebook, WhatsApp, etc. Both have several genuine applications and signify great research openings waiting to be addressed.

REVIEW OF LITERATURE

A new concept called pixel value differencing (PVD) has been proposed by Wu and Tsai [3] in the field of image steganography for gray images. The PVD method divides the total image into smooth and edge areas. The difference value d is calculated between the two pixels. A range table has been specified for the value d. A new difference value d' replaces the old d value to embed the secret data. The width of the range table decides the number of bit that is allowed to embed. This method gives better results in terms of imperceptibility and capacity as compared to LSB techniques. Zhang and Wang [4] noticed that, the original PVD technique proposed by Wu and Tsai [3] is vulnerable to histogram-based steganalysis. That is the stego-image exhibit an abnormal behaviour in the histogram. They proposed a pseudo-random dithering to get dynamic range of values instead of static or fixed range for the blocks. This technique preserves the advantages like capacity of original PVD and also avoids the unusual behaviour shown by the histogram. Hence the security is an added advantage. Chang et al. [7] found that the capacity of the PVD technique presented by Wu and Tsai [3] can be increased further for a gray-level image. There is a gain of 84.16% on average hiding capacity by the overlapping concept proposed by the authors while maintaining satisfactory image quality. A new steganographic method has been proposed by Wang et al [8] to minimize the distortion on the stego-image. The proposed method is the combination of pixel value differencing (PVD) and modulus function. At first the difference value is computed from two consecutive pixels by applying PVD method. The difference value suggests the number of bits to hide. Then by using modulo operation the remainder of the two consecutive pixels is derived, and the secret data are hidden in the pixels by altering the remainder. Experimental results reveal that the use of modulo operation greatly minimizes the distortion and increases the attack resistance. To increase the capacity of original PVD technique proposed by Wu and Tsai[3], a steganographic technique called Tri-Way PVD has been proposed by Chang et al. [9] by using 2×2 pixel blocks with multi-directional differences. It has been experimentally concluded that the capacity and security can be further enhanced compared to the original PVD method. A novel lossless data hiding technique has been proposed by Lin et al [10] by taking three nonoverlapping pixel blocks having two absolute differences called as block difference. Experimentally it has been proved by the authors that the average embedding capacity can be increased. This has been observed that the PVD method introduces distortion to stego-image no matter how much the capacity is reduced. So keeping this in view by avoiding more data embedding to smooth regions Luo et al [11] proposed a new way of embedding secret data to cover image. At first the image is partitioned into small squares. The squares are further made rotation of 0, 90,180, and 270 degrees. The two difference value of three non-overlapping consecutive pixels is calculated and middle pixel is used to hide the secret data. The amount of secret bits will be embedded depending upon the differences among the three non-overlapping consecutive pixels. The proposed technique resists to PVD histogram analysis. Wang et al [8] in 2008 proposed a new direction for data embedding which is the combination of PVD and modulus function. Although good capacity is achieved but the security is not improved. So Joo et al [12] proposed a novel method to improve the stego-image quality which will ensure the security for the secret data. According to them the algorithm is divided into four steps. The first one is the pixel pairing step where the cover image is divided into two consecutive pixels of non-overlapping sub-blocks. Secondly in the embedding step by using the modulus function the pixel value is increased or reduced to match with the message. Thirdly in the adjusting step it solves the out-of-sub-range problem so that there is no variation in the PVD histogram. Finally in the last step, if the pixel value goes beyond the range of 0 to 255 then it will bring back into the range. The results suggest that this method proves to be better compared to Wang et al. [8] in terms of security and capacity. Hong et al [13] proposed a new technique of data embedding using the diamond encoding (DE) technique. A multiple-base notational system (MBNS) has been introduced using modified diamond encoding. The proposed method modifies the diamond encoding to embed in multiple bases and solves the overflow and underflow problem. Experimentally it has been shown that the proposed technique has better embedding capacity and tolerant against RS scheme and histogram analysis steganalysis attack. A new way of data embedding proposed by Mandal and Das [14] which extends the PVD technique to color images. Each pixel have 24 bits contains R, G, B components. All the 3 color components are used for data embedding. Initially the difference value di for each block can be found by di=|pi-pi+1|, where pi and pi+1 are the two consecutive non-overlapping pixels of an cover-image. The difference value determines how many bits will be embedded in which componet of a pixel. Basing upon the contribution of R, G, B components in a color image the maximum secret bits that can be embed in each of R, G, B component of a pixel will be 5, 3, 7 bits respectively. Again for embedding of secret bits it uses the original PVD concept proposed by Wu and Tsai [3]. This results of this schema reveals that better stego-imagequality and security compared to original PVD concept proposed by Wu and Tsai [3] also the falling-off boundary problem can be avoided. In 2012, Lee et al [15] proposed a method which increases the capacity of stego-image. This technique uses the JPEG2000 compression and tri-way pixel value differencing for embedding the secret image. The proposed method is useful for sending large secret image without any distortion. To increase the capacity and security of stego-image, Chang and Tseng [16] proposed a novel technique called two, three, four sided side match method. The pixels are visited in raster scan order. In the two sided side match steganography, let Pxbe the target pixel where secret data will be embedded and gx be the gray value for Px. Let gu and glbe the gray values for the upper pixel Pu and left pixel Pl of a target pixelPx. The difference value d is calculated as d= (gu+ gl)/2 - gx. If the difference value are in the range of -1 to 1 then there is only 1 bit allowed to embed in the LSB bit of the target pixel Px , otherwise, if d >1 then b=log2 |d|, bits are allowed to embed. A new value is assigned to the difference value d and target pixel gx. At times the new value of the pixel Px may fall off the boundary of the range {0, 255}. Any pixel that suffers with fall off boundary problem (FOBP) will be not considered for data embedding. The three sided side match method have three variants. In first variant the three neighbouring pixels such as upper, left and right are used. In variant 2 instead of right the bottom pixels taken along with upper and left. Left-upper, right-upper, left-bottom and right-bottom are taken to find the difference value in case of last variant. Similarly upper, left, right and bottom neighbouring pixels are exploited for secret data embedding in a target pixel in four sided side match method. This method has the clear advantage of more stego-image capacity and better security compared to LSB techniques. The capacity and quality of the stego-image plays a vital role for a stego-image in secret data communication, In this regard Liao et al [17], have proposed a technique called four pixel differencing and modified LSB substitution. In this work the cover image is separated into non-overlapping four pixel blocks having gray values. The average difference value (k) is used to locate the range. The concept of modified LSB substitution is used to embed k-bits of data bits in the pixels located in that block. As this technique is highly inclined towards LSB substitution, so the stego-image has less attack resistance, but the hiding capacity is more. The capacity of stego-image and security of secret data have major role behind the success of any steganographic algorithm. Yang et al [18] suggested a new technique to achieve this. In contrast to Wu and Tsai [3] where a pair of pixels are processed at a time, the authors considered two pair of pixels for processing. There are three ways the four pixels can be grouped. The grouping of pairs of two pixels is done by taking the vertical, horizontal and diagonal pairs. Also to prevent the fall-off boundary problem they proposed a shifting schema. The proposed method avoids the Fridrich et al.'s detection [23] with improved hiding capacity. In case of PVD technique the more the difference values the more the data that can be embedded. But to embed more data so as to increase the capacity sometimes the pixel values cross the boundary values. If the pixel values exceed the boundary values then, this is called fall-off boundary problem. Swain and Lenka [19] marked this issue and then proposed revised variants of two, three and four sided side match with higher embedding capacity. Swain[20] has proposed a steganographic technique using pixel value differencing. There are four different methods and each has their unique idea to find the difference value. In five neighbours differencing method the difference value is calculated by taking the difference of maximum to minimum of gray values among five pixels namely right, upper, left, upper-right, bottom and upper-right corner pixel of a target pixel. In six neighbours differencing method the difference value is calculated by same way as in five neighbour differencing method with one extra pixel as upper-left corner. Similarly for seven neighbours differencing method one extra pixel as bottom left corner and for eight neighbours differencing method one more extra pixel such as bottom left corner. Experimental study shows that the quality of the image is better in case of five neighbours differencing and the capacity is higher in eight neighbours differencing. Pradhan et al [21]proposed a pixel value differencing technique based on PVD called two neighbour method, three neighbour method and four neighbour method. The result reveals that the capacity is good in four neighbour method with acceptable stego-image quality. An adaptive pixel value differencing method using vertical and horizontal edges has been proposed by Swain [22]. Two techniques is given as first one uses 2×2 pixel blocks and second one uses 3×3 pixel blocks. The first technique offers good capacity and second one provides good stego-image quality.

REFERENCES

[1] Anderson RJ, Petitcolas FAP. On the limits of steganography. IEEE Journal on Selected Areas in Communications. 1998; 16(4): 474-481. [2] Johnson NF, Jajodia S. Exploring steganography: seeing the unseen. IEEE Computer Journal. 1998; 31(2): 26-34. [3] Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters. 2003; 24: 1613-1626.

[4] Zhang X, Wang S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognition Letters. 2004; 25: 331-339. [5] Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEEE Proceedings on Vision, Image and Signal Processing. 2005; 152(5) 611-615.

[6] Yang CH, Weng CY, SJ. Wang, Sun HM. Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems. The Journal of Systems and Software. 2010; 83: 1635–1643.

[7] Chang CC, Chuang JC, Hu YC. Spatial Domain image hiding scheme using pixel-values differencing. FundamentaInformaticae. 2006; 70: 171–184.

[8] Wang CM, Wu NI, Tsai CS, Hwang MS. A high quality steganographic method with pixel-value differencing and modulus function. The Journal of Systems and Software. 2008; 81: 150.-158.

[9] Chang KC, Chang CP, Huang PS, Tu TM. A novel image steganographic method using tri-way pixelvalue differencing. Journal of Multimedia. 2008; 3(2): 37-44.

[10] Lin CC, Hsueh NL. A lossless data hiding scheme based on three-pixel block differences. Pattern Recognition. 2008; 41: 1415 – 1425.

[11] Luo W, Huang F, Huang J. A more secure steganography based on adaptive pixel-value differencing scheme. Multimed Tools Appl. DOI 10.1007/s11042-009-0440-3. 2010: 407-430.

[12] Joo JC, Lee HY, Lee HK. Improved Steganographic Method Preserving Pixel-Value Differencing Histogram with Modulus Function. EURASIP Journal on Advances in Signal Processing. doi:10.1155/2010/249826. 2010: 1-13.

[13] Hong W, Chen TS, Luo CW. Data embedding using pixel value differencing and diamond encoding with multiplebase notational system. The Journal of Systems and Software. 2012; 85: 1166-1175.

[14] Mandal JK, Das D. Color image steganography based on pixel value differencing in spatial domain. International Journal of Information Sciences and Techniques. 2012; 2(4): 83-93.

[15] Lee YP, Lee JC, Chen WK, Chang KC, Su IJ, Chang CP. High-payload image hiding with quality recovery using tri-way pixel-value differencing. Information Sciences. 2012; 191: 214-225.

[16] Chang CC and Tseng HW. A steganographic method for digital images using side match. Pattern Recognition Letters. 2004; 25: 1431-1437.

2/16/2024