Grenze International Journal of Engineering and Technology, Jul 2019

Secure Data Transmission through Digital Protection Wall based on RGB Color Model in Wireless Network

Ms. Devika Gawande[1] and Dr. S. W. Mohod[2]
[1]Research Scholar, Dept. of Electronics, Prof. Ram Meghe Institute of Tech.& Research, Badnera-Amravati, India
Email: gawande195@gmail.com
[2]Professor, Dept. of Electronics, Prof. Ram Meghe Institute & Tech.& Research , Badnera-Amravati, India
Email: sharadmohod@rediffmail.com

***Abstract*—Wireless communication provides the mean of connectivity to everyone, everywhere and need to have more attention on security. The secrecy and security of information has always been important to the people whenever it come to confidential data. Today there is advancement in internet technology and there has been increase use of text and multimedia data transfer over internet. The paper suggests to provide an additional layer of security to secrete data transmission, which hides the confidential information within carrier. The carrier used is the images that can hide secret information within the region of image. The paper proposed a method of half toning visual cryptography technique with digital protection wall. It improves thee perceptual quality as well as capacity of carrier by considering higher LSB layer for hiding secret information and replacing RGB component bit with secret information. The data is extracted simply by using reverse algorithm and the capacity, imperceptibility is compared by using various factors like cross correlation, MS error, peak to signal noise ratio. The suggested protection wall is flexible so that carrier can hide the data within the protected area and shall protect from unauthorized user which will be known to receiver only.**

***Index Terms*— Carrier Image, Digital Protection Wall, Half Toning Visual Cryptography.**

I. INTRODUCTION

Data hiding is the transmission of a secret message hidden within an ordinary carrier without revealing its existence. The container/cover file may be a digital still image, audio file or media file. Once the secret message has been embedded, it may be transferred across insecure lines or posted in public places as per security policy. Usually, the data rate of covert data transmission using data hiding is low in order to keep the covert data imperceptible within the cover medium. This data rate is somewhat proportional to the volume of the cover medium. For such reason, digital media is a convenient choice for data hiding. Nowadays, with given high degree of collaboration and cooperation in modern information systems such as emerging multimedia sensor networks, covert communications become a greater threat to forensic analysis than ever. It is imperative to investigate methods to detect and discourage covert communications such as data hiding in multimedia networks that acquire highly correlated data [1]-[9].

The proposed data hiding scheme uses half toning visual cryptography to hide the data inside the carrier as image. The proposed data hiding scheme set digital protection wall inside the carrier and the secrete data is encoded inside the wall, as to provide another layer of security to the secrete data. Even if data loss occurs it

Grenze ID: 01.GIJET.5.2.505

won't affect the secret data. Also, the proposed technique makes the use of higher LSB for replacement with secret data, in order to make data secure from unauthorized user.
The method of visual cryptography is used to hide secrete data inside the carrier and it has important features

- The primary focus is to add another layer of security to the secrete data.
- This additional layer is nothing but digital protection wall within its boundaries secrete data is hided.
- Design protection wall is very much flexible so that user can set its own protection wall boundaries and hide the data within that.

II. DATA HIDING TECHNIQUES

The existing data hiding techniques are methods are stenography, cryptography and watermarking, each has its own merits and demerits, radically all data hiding should follow the properties like high capacity, robustness, security, payload and reliability. For the degree of security of data transfer certain method can be applied and stated as follows.

A. Stegnography

It involves concealing of secrete information within ordinary file in order to avoid detection to unauthorized user. Because if secrete data in revealed by unauthorized user it loses its originality. Therefore, in that case it become necessary to make data undetectable to unauthorized user. Steganography is a Greek word in which stegano means hidden and graph means to write. Stegnography involves a cover file. Within this cover file secrete information is embedded. This cover can an audio, video or image and secrete information can also be any form like text, doc file etc. Hence by using this technique of steganography the secrete data is transmitted over wireless medium without getting detected by unauthorized user [17]-[18]. Steganography can be performed by using the least significant bits in image files, placing comments in the source code, altering the file header, spreading data over a sound file's frequency spectrum, or hiding encrypted data in pseudorandom locations in a file.

B. Cryptography

The main objective of Cryptography is to protect user's integrity and confidentiality from unauthorized access and securing the secrecy of communication using methods like encryption and decryption. The key idea behind the secure transfer of message in Cryptography is based on the principle of message scrambling, so it cannot be easily detectable by malicious people.Cryptography techniques can be basically classified into two types. Symmetric-key cryptography and Asymmetric-key cryptography. In Symmetric-key, only one key is used by the sender as well as the receiver. In Asymmetric-key, two different keys are used: a public key which is disclosed to all and a private key which is secretly known only to the authorized recipient of data. In Cryptography, even though the secret data is sent in the unreadable format, it gives the hint of existence of secret data to the unauthorized recipient [14].

C. Digital Watermarking

It is method of embedding data into digital media content. This method is generally used to verify the credibility of content or to recognize the identity of digital content owner. Here Watermarking means to impressed either text or image onto the paper to provide its evidence of authenticity. Then the term digital watermarking came to existence. In case of digital watermarking bits are inserted into the digital media (image, video or audio) to identify the right. The main goal of digital watermarking is to hide message into digital media so as the new data obtained after hiding is practically indistinguishable to unauthorized user so that it cannot replace or remove the original content [6].

D. Encryption

Basically, encryption is used to convert secrete data into the form which is unidentified to unauthorized user. Encryption involves algorithm which covert the information into other form so that only indented user can understand. At the receiver side, receiver must know the hiding algorithm in order to obtained the secrete data which was encrypted at the sender side. But simply applying encryption algorithm and extracted the data at receiver side leaves many problems unsolved, once it was sent over wireless media [9]-[10]

E. LSB Replacement

In this method, LSB is replaced to hide secrete data. Generally, in this case carrier which is used to carry secrete data can be image, video or audio. But in case of grey scale image each pixel is represented in terms of bits. The

last bit within this is called Least Significant Bit, as its value affect the pixel value only by '1'And hence this property is used to hide secrete data in it. This technique of data hiding takes much more time to embed the secrete data but provide much high level of security. As today hacker has become more mastermind this type security to secrete data now can be easily identified by them.[11]-[17].

The main focuses on maximizing security and capacity factor of data hiding. The confidential communications over public networks can be done using digital media like text, images, audio and media on the internet. Simply hiding the contents of a message using cryptography was not adequate. Hiding of message should provide an additional layer of security. To provide the more security the authors suggested the new procedures in data hiding for hiding ciphered Information inside a digital color bitmap image[4]-[7] . Researcher also use quadratic method depending on the locations concluded by the binary image, beside of public key cryptography,the conjunction between cryptography and data hiding produce immune information.

Researcher [18] proposed a new framework of reversible Data Hiding in encrypted JPEG bitstream which makes the use of visual on JPEG carrier. But problem with such type of media data is that it changes carrier perceptual quality. Also, this method is not practical for cloud storage. Another method of media data hiding is to use grayscale invariance method [2] . It only used red and blue component for concealing the data. Rather than using complete channel ang grey channel value is adjusted to maintain the originality of the carrier. But drawback of this technique is that it disturbs the carrier media after data hiding as complete channel capacity is not used to hide the data [13]-[20].

III. A Proposed System Architecture

The basics of data hiding rely on three different facts i.e. capacity, security, and robustness. Capacity means the media on which the data is to be hidden should hold the data, so that the complexity of the medium should not be disturbed. Security means the embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks. Finally, robustness means the amount of manipulation a cover image (original image) can handle without drawing any attention that a change has taken place. The proposed system architect makes the use of half toning visual cryptographic technique and the system architect is shown in Figure 1. The propose technique uses simply LSB of the carrier image component uses higher LSB. The extraction of data on the other side is also simple because it involves less calculation while retrieving the data and hence propose to use higher LSB to encode the data.

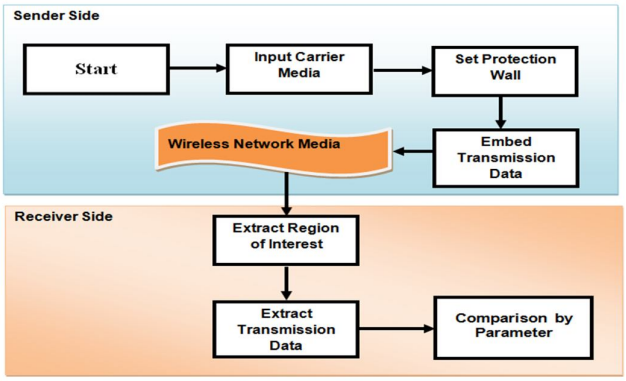

Figure 1: Two tier Architecture of Proposed System

The two-tier architecture of proposed system deal with processing of data on two sides namely , at the sender side and also at the receiver side. On the sender side, the user has to select carrier in which secrete data is to be hided. The carrier used in the system is an Image. We can also use video or audio stream for the purpose of data hiding but problem arises with these media that it is very easy to detect small change done with these carriers so here image is used as carrier. At the sender side, after selecting appropriate carrier, the digital protection wall limits are to be set. The limits of digital protection wall are chosen in rectangular frame. Hence rectangular frame is taken into consideration so that only two parameters are required for setting the required limits of wall on top rightmost and the bottom leftmost.

In order to hide the data inside the region of interest, ROI it is necessary to fetch the pixels within this region. After fetching component within this region, the secrete data which we want to hide is then converted into binary

form. Then the required position of bit which we want to replace by secrete data is chosen. The chosen position of bit , the corresponding bit of RGB component is replaced with secrete data bit. In this way embedding of confidential data inside the carrier having protection wall is carried out.

At the receiver side, the user needs to follow simple steps in order to decode exact data which was embedded at the sender side. After receiving the carrier with secret data user needs to select the protection wall limit in order to extract the ROI in which the data is embedded. After extracting the ROI from protection wall limits, the conversion of binary to ASCII is carried out. Once this conversion is done then system compare the results by different parameter such as MSE, PSNR, and structural content of received carrier in order to determine the perceptual quality of carrier at the other side.The flow chart on sender and receivwer side is shown in Figure 2 and Figure 3.

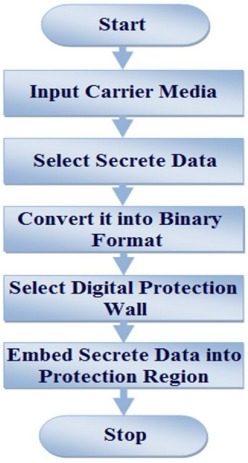

Figure 2: Flowchart of Sender side

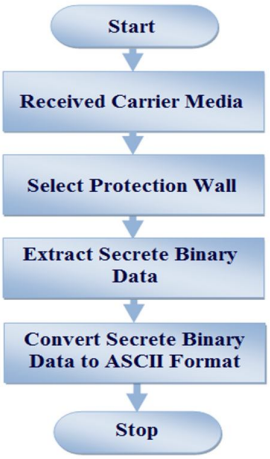

Figure 3: Flowchart of Receiver Side

A. Calculate the embeding capacity

The embedding capacity of the carrier plays important role as it provides information to user that how much data can be embedded within the single carrier. Consider a carrier of height 'H' and width 'W' , the embedding capacity can be calculated as simply as (1)

$$I(size)=H*W \quad (1)$$

Where I(size) represents the carrier capacity.

B. Set digital protection wall

The important component of proposed system is the digital protection wall as it adds another layer of security to the secret data. Here the term 'Protection Wall is used as it acts as a barrier between the carrier information and secretes information making it imperceptible to unauthorized user. The protection wall concept or the boundaries of the wall can be chosen according to the users need and the position where user want to hide the data.

While setting protection wall the system needs to co-ordinate points as (x1,y1) and (x2,y2) such that the protection wall is set with in the rectangular frame. But there are few conditions while selecting these coordinate points so that the secrete data remain intact and less quantization error occurs.

These conditions are given as (2)

$$P1=\{x1, y1\}\ P2=\{x2, y2\} \quad (2)$$

Where P1 and P2 represents pixels of image

Protection wall (3) set as

$$Pw=region|x2-x1, y2-y1| \quad (3)$$

Where,

x2 >x1-------Valid regionx1 > x2-------Invalid region

y2 >y1-------Valid regiony1 > y2-------Invalid region

These conditions are necessary to satisfy while setting protection wall in order to make data imperceptible to the unauthorized user. The carrier image is shown in Figure 4.

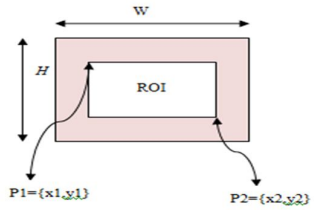

Figure 4.Carrier Image

C. The ROI calculation

The ROI is calculated simply by taking x and y coordinates which is given as x 2 , y2

The Region of interest is shown in (4) as ROI=∫ ∫ P i,j , Pi,j+1 ,Pi,j+2--- ---- ---,Px2,y2 (4)

Image as in (5) ,capacity (6) &(7), I =x1 j=y1 (5)

Capacity = (x2-x1)*(y2-y1) (6)
Capacity max= (x2-x1)*(y2-y1)*3 bits (7)

D. Classification of Bits

Image is basically composed of pixels and each pixel consist of three component 'RGB' i.e. Red component, Blue component and Green component. Figure 5 shows how each component is used to store secrete data inside the region. The shaded region represent the ROI within the three components where actual data is hided.

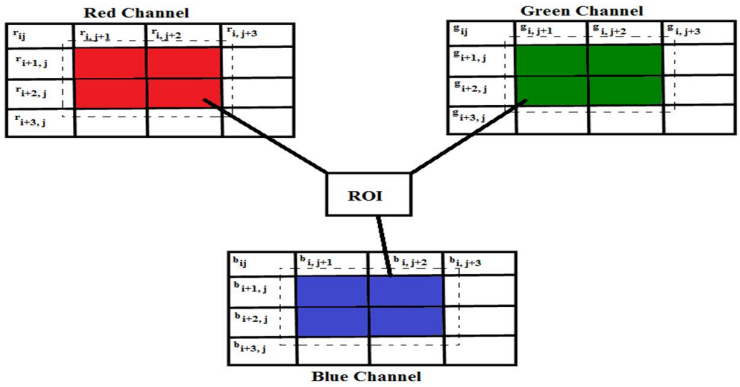

Figure 5: ROI within RGB Component

Each pixel is represented by one '8 bit'byte. Thus the maximum number of colors that can be displayed at any one time is 256.Hence these are used to store the secret data in the proposed work higher LSB is chosen for the purpose of data hiding. When particular higher LSB bit i.e. 5th, 6th or 7th bit position is selected to hide the data, the classification of bit is carried out. Here classification named as 'Class 0' and 'Class 1'.
'**Class 1**' contain all the component of ROI that have **bit 1** at particular position of bit which is selected for replacement to hide secret data, same as case for **'Class 0'**.Flow chart of data hiding is shown in Figure 6.
According to above flow, if bit of BSD is **0**and component is also found within the same class, then there is no need to replace the bit with BSD. But the BSD is not found within the Class 0, then closest match is found out within the same class and then replacement of BSD is carried out.

E. Data Hiding Algorithm

The data hiding algorithm is developed and shown in Figure 7.In the above data hiding algorithm Sd represents the 'secrete data 'if the secrete data bit is 0 and corresponding position bit within the component is also 0 then there is no replacement, otherwise find the closest match within the class 0. Similar process repeat for class 1.

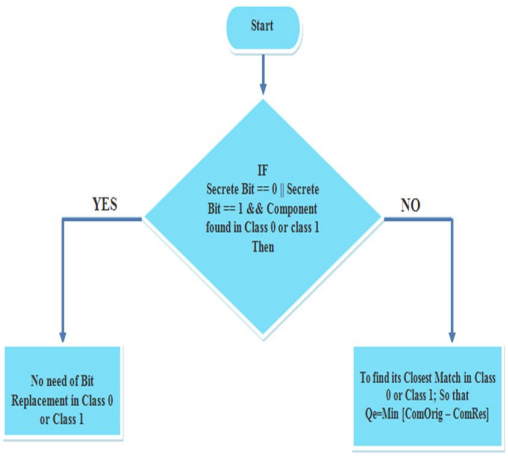

Figure 6: Shows flow of Data Hiding in Class 0 and Class 1

Algorithm:
Step 1: Start
Step 2: Input the secrete data(Sd)
Step 3: Load classes(0,1)
Step 4: For i=1 to length(Sd)
If Sd(position)==0
Find the best fit in Class 0 and replace in image
Else
There is no replacement
End
If Sd(position)==1
Find best fit in class1 and replace in image
Else
There is no replacement
End
End
Step 5: Save the result image
Step 6: Stop.

Figure 7. Data Hiding algorithm

F. Data Extraction process

Once the data is hided within the carrier it is then transferred over wireless media. At the receiver side the extraction is carried out which is nothing but a reverse process of embedding the data. While extracting the data the user at the receiver side will require 3 things

- No. bits encoded within the carrier
- Position of bit which is altered i.e. classification bit
- Protection wall limits

Once user gets all the above information then and only then it is possible to extract the original data which is hided at the sender side. These conditions provide more security to the secrete data as only intended user will know the conditions to decode the data.

IV. Experimental Results

The experimental results are to focus on the various parameters i.e. entropy, mean intensity, time required for encryption and decryption, peak signal to noise ratio, mean square error. On performing various operations on the test image, it gives result of RGB and Gray component of image , shown in Figure 7 and quantization error in Figure 8.

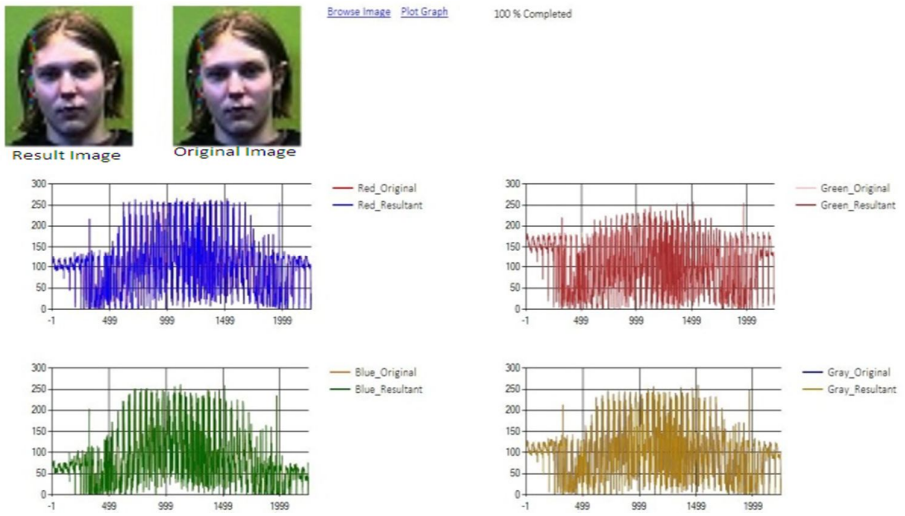

Figure 7 RGB and Gray component

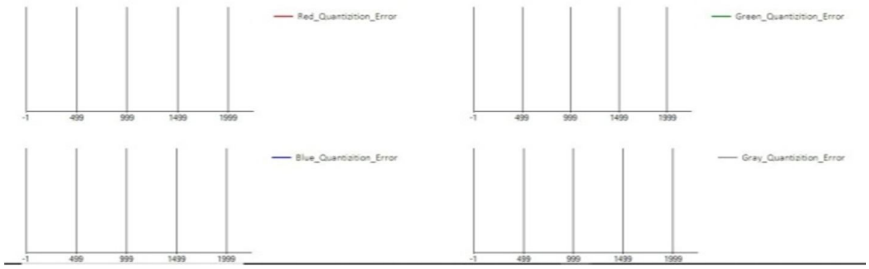

Figure 8: Zero Quantization Error of RGB component

From the figure 8, it is clear that the proposed system generates almost 0 quantization error while extracting the data and hence it is more beneficial to transfer the data with this system. It is clear that that the visual perceptual quality of image is as it, there is no change or difference between the two carriers. These carriers image having parameters which are as in Table I. Resultant of Image parameter in Table II.

TABLE I. INDIVIDUAL IMAGE ANALYSIS

Image Type	Red-Mean	Green-mean	Blue-mean	Mean	Pure Height	Pure Width	Entropy
Original Image	105	108	81	221586	50	45	449.33
Resultant Image	105	108	81	221586	50	45	449.33

TABLE II. RESULTANT IMAGE ANALYSIS

Parameter	Avg-Red	Avg-Green	Avg-Blue	MSE	PSNR	Normalize Absolute Error	Cross Correlation	Structural Content
Value	0	0	0	0	ω	0	1	1

V. CONCLUSIONS

A modified method of data hiding is implemented using two tire architect system in order to enhance the security of data. In propose system the binary secret data is hidden inside carrier image using half toning visual cryptography; security of data is further enhanced by setting digital protection wall inside the carrier in which the secret data is hided. The suggested method ensures high security of secret data by using Higher LSB bits for hiding the binary secret data. Carrier with secret data is then sent separately over the network. If the intruder intercepts image and tries to extract the secret data then he/she will be able to recover the data only partially. Thus this method ensures the lossless recovery of the secret image at the receiver end.From the parameter it is very clear that MSE is 0 and PSNR is much higher indicating the higher perceptual quality of resultant carrier image. Also the structural content is 1 indicating there is no change in quality of image after embedding. Hence, is better approach to transfer the secrete data over unsecure lines.

REFERENCES

[1] Thanikaiselvan V, Bansal T, Jain P, Shastri S. IWT Domain data hiding in image using adaptive and non adaptive methods. Indian Journal of Science and Technology. Vol. 9(5), Feb.2016.
[2] Y. Miura, X. Li, S. Kang and Y. Sakamoto, "Data hiding technique for omnidirectional JPEG images displayed on VR spaces," 2018 International Workshop on Advanced Image Technology (IWAIT), Chiang Mai, pp. 1-4.,2018.
[3] D. Hou, W. Zhang, K. Chen, S. Lin and N. Yu, "Reversible Data Hiding in Color Image With Grayscale Invariance," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 29, no. 2, pp. 363-374, Feb. 2019.
[4] Andreas Westfield and Gretta Wolf," Data hiding in a Media Conferencing System", Information Hiding 1998, LNCS 1525, pp. 32-47, 1998.
[5] L. Robert, T. Shamuyarira, "A Study on Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.
[6] D. P. Gaikwad and Dr. S.J. Wagh, "Color Image Restoration for Effective Data hiding", i-manager's Journal on Software Engineering, Vol. 4, No. 3 , pp.65-71, March 2010 .
[7] W. Bender, D. Gruhl and N. Morimoto, "Technique for data hiding", IBM System Journal, Vol.35, NOS 3, 1996.

[8] Sandip Thitme and Vijay Kumar Verma, “A recent study of various encryption and decryption techniques,” International Research Journal of Advanced Engineering and Science, Vol.1, Issue 3, pp. 92-94, 2016.
[9] Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Vol. 13 Issue 15 , 2013.
[10] S. Suma Christal Mary, “Improved Protection In Media Steganopgraphy Used Compressed Media Bitstream,” International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766,
[11] Fahim Irfan Alam et. al. "An Investigation into Encrypted Message Hiding through Images using LSB", International Journal of Engineering Science and Technology, vol. 3, No. 2, Feb 2011.
[12] Hemalatha S, U Dinesh Acharya, "Comparison of Secure And High Capacity Color Image Steganography Techniques ", International Journal of Advanced Information Technology (IJAIT) Vol. 3, No. 3, June 2013.
[13] H.A. Patil, P. Saxena, "Analysis and Review of the Steganographic Techniques", International Journal of Computer Sciences and Engineering, Vol.-6, Issue-11, Nov 2018.
[14] S. Jeevitha1 and N. Amutha Prabha, "A Comprehensive Review on Steganographic Techniques And Implementation", ARPN Journal of Engineering and Applied Sciences, Vol. 13, NO. 17, September 2018
[15] Zhenxing Qian, Haisheng Xu, Xiangyang Luo, Xinpeng Zhang, "New Framework of Reversible Data Hiding in Encrypted JPEG Bitstreams", IEEE, Transactions on Circuits and Systems for Video Technology, 2018,
[16] Mohammed A. Saleh, "Image Steganography Techniques - A Review Paper", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 9, September 2018.
[17] Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, June 2010.