ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

A PROPOSED METHOD IN IMAGE STEGANOGRAPHY TO IMPROVE IMAGE QUALITY WITH LSB TECHNIQUE

Krati vyas[1], B.L.Pal[2]

M.tech student, Department of C.S.E, Mewaruniversity, Chittorgarh, India [1]

Asst.Professor, Department of C.S.E, Mewar University, Chittorgarh, India [2]

Abstract: Image steganography is becoming an important area in the field of steganography. As the demand of security and privacy increases, need of hiding their secret information is going on. If a user wants to send their secret information to other persons with security and privacy he can send it by using image steganography. During the last few years lot of different methods of hiding information has been done in this field. Some of the existing methods for hiding information give good results only in case of information gets hidden successfully.

LSB is the most popular Steganography technique. It hides the secret message in the RGB image based on it its binary coding. LSB algorithm is used to hide the secret messages by using algorithm. LSB changes the image resolution quite clear as well as it is easy to attack. It is clear that LSB changes the image resolution when the least significant bits add in the binary image format, so that image quality become burst and there become so much difference in the original image and encoded image in the respect of image quality.

So to overcome this problem, In this thesis I suggested modifying the LSB technique so that we can get same image quality as it has before the encoding. The basic idea to get good image quality, I am going to modify the hiding procedure of the least significant bit. In this step I will hide two bits by two bits by taking identical values.

Keywords: LSB, RGB

I. INTRODUCTION

A. Stegnography

Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message by using certain cryptographic algorithms for converting the secret data into unintelligible form. On the other hand, Steganography hides the message so that it cannot be seen [1].

In the other words, we can say that steganography is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party [2].

The basic structure of Steganography is made up of three components: the "cover medium", the hidden message, and the key. The cover medium can be a painting, a digital image, an mp3, even a TCP/IP packet among other things. It is the object that will 'carry' the hidden message. A key is used to decode/decipher/discover the hidden message. This can be anything from a password, a pattern, a black-light, or even lemon juice. The following formula provides a very generic description of the pieces of the steganographic process:

Cover medium + hidden data + stego key = stego medium

In this context, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files.

"Steganography's niche in security is to supplement cryptography, not replace it. If a hidden message is encrypted, it must also be decrypted if discovered, which provides another layer of protection."

B. Steganalysis

Steganalysis is the process of identifying steganography by inspecting various parameter of a stego media. The primary step of this process is to identify a suspected stego media. After that steganalysis process determines whether that media contains hidden message or not and then try to recover the message from it.

In the cryptanalysis it is clear that the intercepted message is encrypted and it certainly contains the hidden message because the message is scrambled. But in the case of steganalysis this may not be true. The suspected media may or may not be with hidden message. The steganalysis process starts with a set of suspected information streams [3]. Then the set is reduced with the help of advance statistical methods.

II. LITERATURE REVIEW

A. Earlier Techniques of Steganography

The common modern technique of steganography exploits the property of the media itself to convey a message.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

The following media were the candidate for digitally embedding message:

- Plaintext
- Still imagery
- Audio and Video
- IP datagram.

Plaintext steganography

In this technique the message was hide within a plain text file using different schemes like use of selected characters, extra white spaces of the cover text etc.

Use of selected characters of cover Text.

Sender was sent a series of integer number (Key) to the recipient with a prior agreement that the secret message was hidden within the respective position of subsequent words of the cover text. For example the series was '1, 1, 2, 3, 4, 2, 4,' and the cover text was **"A team of five men joined yesterday"**. So the hidden message is **"Atfvea"**. A "0" in the number series was indicated a blank space in the recovered message [3]. The word in the received cover text was skipped if the number of characters in that word was less than the respective number in the series (Key) which was also be skipped during the process of message unhide.

Use of extra white space characters of cover text.

A number of extra blank spaces were inserted between consecutive words of cover text. This numbers were mapped to a hidden message through an index of a lookup table. For example extra three spaces between adjacent words were indicated the number "3" which subsequently indicates a specific text of a look-up table which was available to the both communicating parties as a prior agreement [3].

Still imagery steganography

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS could not detect the variation in luminance of color vectors at higher frequency side of the visual spectrum. A picture can be represented by a collection of color pixels. The individual pixels could be represented by their optical characteristics like 'brightness', 'chroma' etc. Each of these characteristics could digitally expressed in terms of 1s and 0s.

For example: a 24-bit bitmap had 8 bits, representing each of the three color values (red, green, and blue) at each pixel. If we considered just the blue there were come out 28 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity was likely to be undetectable by the human eye. Hence, if the terminal recipient of the data was nothing but human visual system (HVS) then the Least Significant Bit (LSB) can be used for something else other than color information [3]. This technique could be directly applied on digital image in bitmap format as well as for the compressed image format like JPEG. In JPEG format, each pixel of the image was digitally coded using discrete cosine transformation (DCT). The LSB of encoded DCT components could be used as the carriers of the hidden message. The details of above techniques were explained below:

Modification of LSB of a cover image in 'bitmap' format.

In this method binary equivalent of the message (to be hidden) is distributed among the LSBs of each pixel. For example we tried to hide the character 'A' into an 8-bit color image [4]. We had taken the eight consecutive pixels from top left corner of the image. The equivalent binary bit pattern of those pixels might be like this: -

00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111

Then each bit of binary equivalence of letter 'A' i.e. **01100101** were copied serially (from the left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern became like this: -

00100110 11101001 11001001 00100110 11001000 11101001 11001000 00100111

The only problem with this technique was that it was very vulnerable to attacks such as image compression and formatting.

Applying LSB technique on DCT

The following steps were followed in this case: -

(i) The Image was broken into data units each of them consists of 8 x 8 block of pixels.
(ii) Working from top-left to bottom-right of the cover image, DCT was applied to each pixel of each data unit.
(iii) After applying DCT, one DCT Coefficient was generated for each pixel in data unit.
(iv) Each DCT coefficient was then quantized against a reference quantization table.
(v) The LSB of binary equivalent the quantized DCT coefficient replaced by a bit from secret message.
(vi) Encoding was then applied to each modified quantized DCT coefficient to produce compressed Stego Image.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Figure **Ошибка! Текст указанного стиля в документе отсутствует.**.1: Example of still imagery steganography. Left hand side image is the original cover image, whereas right hand side embedding a text file into the cover image make the stego image.

Audio and Video Steganography

In audio steganography, secret message was embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There were several methods available for audio steganography.

III .PROBLEM STATEMENT

As we know that steganography is a message hiding technique so that a user can send or communicate to the other user about their secret message securely.

LSB is one of the most popular technique which is used for hiding the secret message. LSB hiding technique works as it hides the secret message directly in the least two significant bits in the image pixels, which affects the image resolution, due to this it reduces the image quality and make the image easy to attack.

Therefore there may be one possibility to remove this problem and make the secret message more secure and enhance the quality of the image is proposed. The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels. By using this proposed method the image will remain same after encoding or hiding the secret message in the image. It will not affect the image resolution.

A. Problemformulation

In the previous chapter we have discussed several steganography techniques, but in this thesis I will give concentration on LSB technique.

Least Significant Bit hiding technique

LSB is the most popular Steganography technique. Many carrier messages can be used in the recent technologies, such as Image, text video and many others. LSB uses the image as carrier message because the image file is the most popular for this purpose because it easy to send during the communication between the sender and receiver. It uses the RGB color image as carrier message. The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels. It hides the secret message in the RGB image based on it its binary coding. Figure 3.1 presents an example about pixel values and shows the secret message. LSB algorithm is used to hide the secret messages by using algorithm. LSB makes the changes in the image resolution quite clear as well as it is easy to attack.

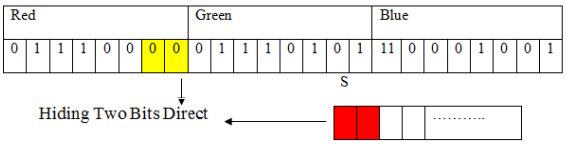


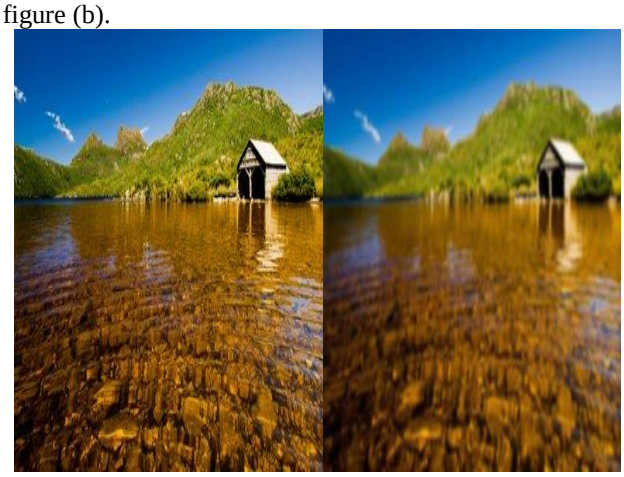
Figure **Ошибка! Текст указанного стиля в документе отсутствует.**.2: Least Significant Bit Hiding Technique

From the above figure it is clear we are hiding two least significant bits directly. But they occurs a problem when we hide these two least significant bits in the image, the resolution of the image becomes blur. So that there become a difference between original image and encoded image. The quality of the image does not remain same after hiding these bits. This is the main problem of LSB technique.

I want to overcome the LSB technique from this problem so I am going to propose a modification in LSB by which this problem will remove from this technique. The basic idea of my propose method is that choose one pixel of the image randomly, select this pixel as the centre of the image and divide the image into three parts Red, Green and Blue parts separately according this centre pixel. Now hide two by two bits of the secret message in each part of the pixel by searching about the identical, if the identical found or satisfied then set the image with new values if the identical does not find, hide in the two least significant bits and set the image with new values. Now save the location of the hiding bits in binary table. This modification will give the same image quality as original image after the encoding.

IV. EXPERIMENTAL RESULTS

LSB technique performs the task to hide the data. Now we implement it on a image by using matlab system. In the following figure there are two images, the figure (a) is showing the original image in which we have to hide the our secret data. Now load this original image in the system and perform all the LSB technique's step one by one to hide the data in this image. When we successfully complete all the steps, we can see the encoded image in figure (b).



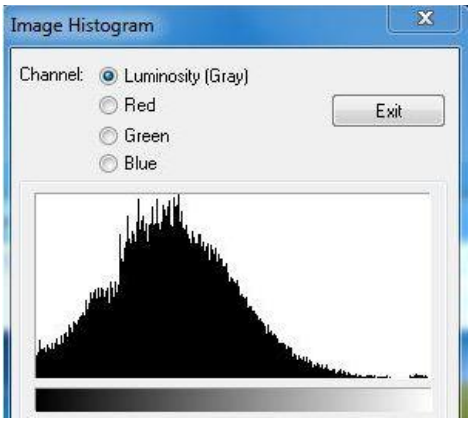
(a) Image (b) Image

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

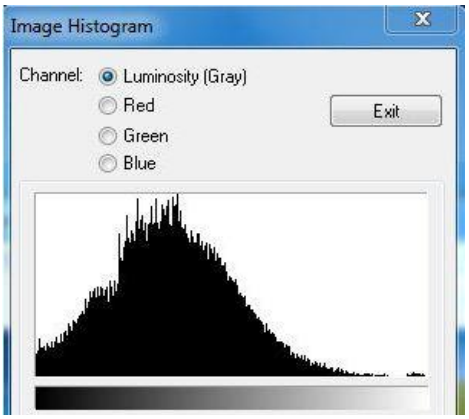
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Now give a attention on both images original and encoded image we can clearly see the difference between the original image and encoded image. Encoded image is that image which has the secret data by performing the LSB technique. The resolution of the encoded image is burst from the original image.

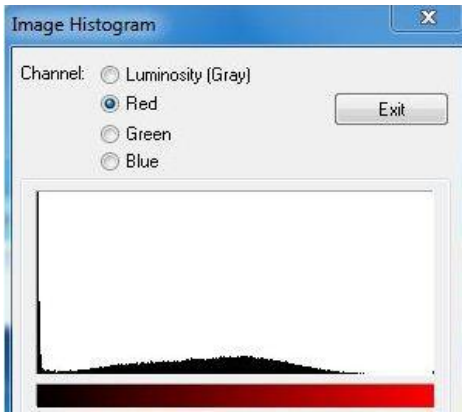
The difference between the original image and encoded image can also see from the following histograms of the both original image and encoded image by using LSB technique in Gray and RGB formats.



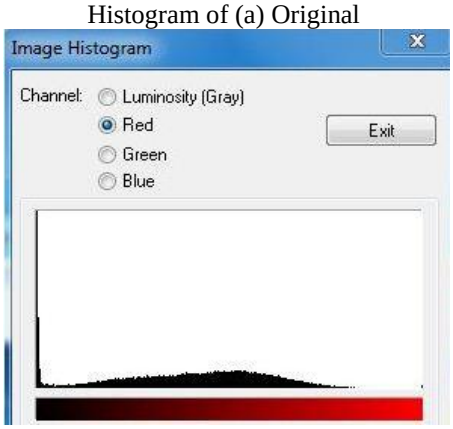
Histogram of (a) Original



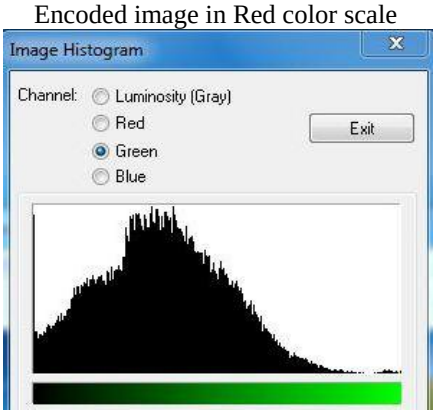
Encoded image in Gray scale



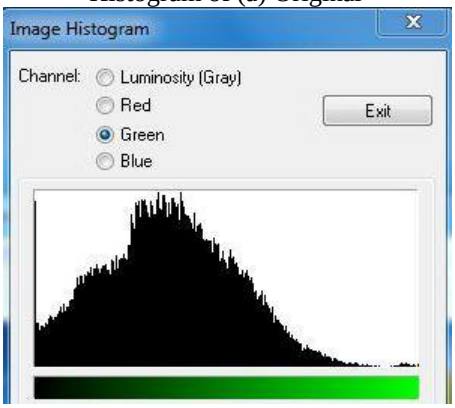
Histogram of (a) Original



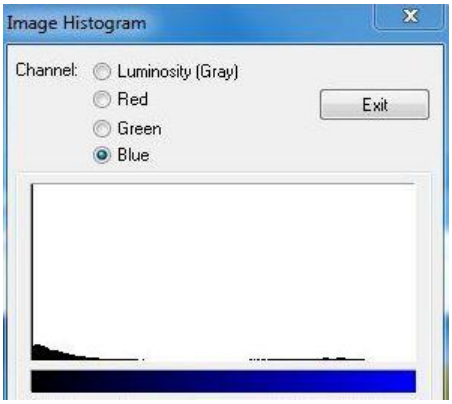
Encoded image in Red color scale



Histogram of (a) Original



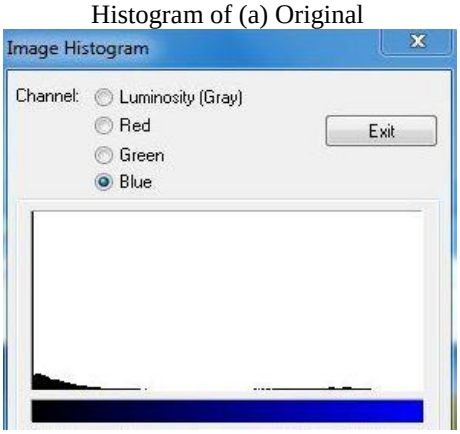
Encoded image in Green color scale



ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

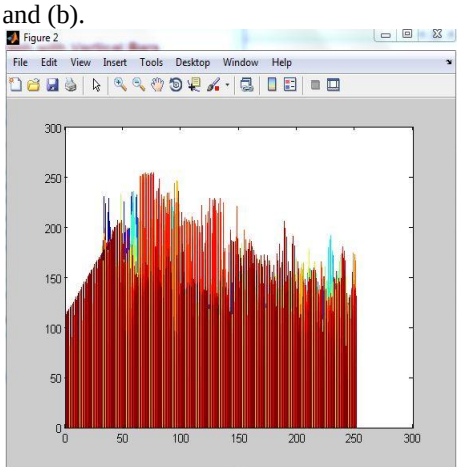
Histogram of (a) Original



Encoded image in Blue color scale

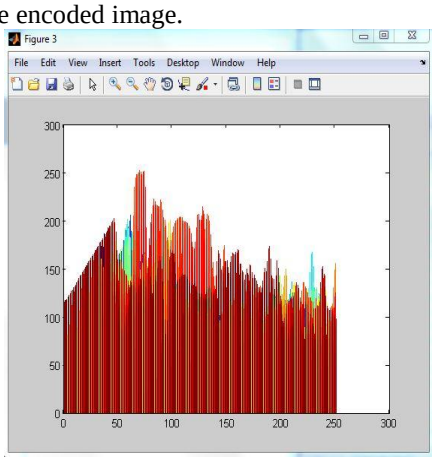
A. Results

The following figure 6.12 shows the bar plot of the original image. When we hide the secret data in the original image by using LSB technique and proposed method it gives the following results, which shows figure 6.13 (a) and (b).

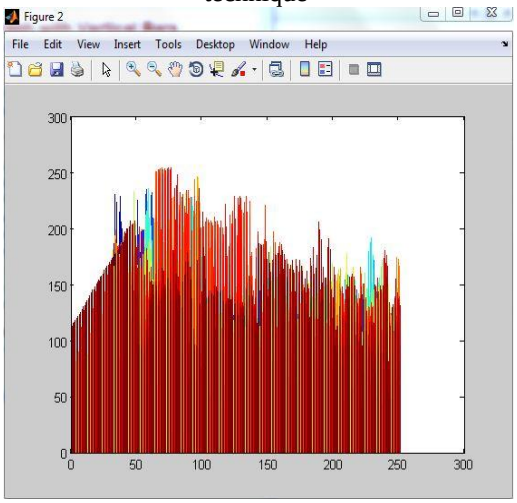


Bar plot of the original image

Now compare the bar plot (figure a) of the encoded image by using LSB technique. We can see that there are so many places on the bar plot of encoded image, which create differences between the original image bar plot and that of the encoded image.



Bar plot of the encoded images (a) by using LSB technique



Bar plot of the encoded images by using proposed technique

Now compare the bar plot(figure b) of the encoded image which comes out by using proposed method to that of the original image. We can see that bar plot of the original and encoded image is about same.

Now from the above experiments, we select an image as original image and performs LSB hiding technique on that image for hiding the secret data or information and after encoding the original image, we compare the both images original and encoded image we find the difference between them. After that we draw the histogram of both original and encoded image in different color scales we find the difference between them and now we draw the bar plot of both original and encoded images we also find difference here between them. So that from these results we easily say that when we apply LSB technique on an image it affects the resolution of the original image after encoding.

If we talk about the proposed method in the experiments we can see the encoded image is about same as original image and when we draw the histograms of both images in different color scales, all histograms are also about same of the original image and encoded image. At finally we draw the bar plots of original image and encoded image we can see that both bar plots are about same. While in all the experiments we find the opposite results when we compare these all experiments with taking encoded image by using LSB technique to the original image.

So finally from the whole discussion we can say that LSB technique affects the resolution of an image when it applies to the original image for hiding the secret data while here we can also see that the proposed method does affect the resolution of an image when it applies on an original image for hiding the data.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

V. CONCLUSION AND FUTURE SCOPE

A. Conclusion

A new Steganography technique was presented, implemented and analyzed. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels.
The proposed method is more efficient, simple, appropriate and accurate than LSB method, it search about the identical then start hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure. This thesis work concluded that the LSB hiding method is the worst case of the proposed method.

B. Future Scope

In our thesis work we propose a new approach which give good quality of the image after encoding the original image by using the LSB technique because LSB technique has a drawback it affects the resolution the original image after encoding, so that image quality go burst. The future work on this project is to improve the compression ratio of the image to the text. The main intention of the project is to develop a steganographic application that provides good security. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible.

REFERENCES

[1] "*Data Hiding in Digital Images: A Steganographic Paradigm*" M.Tech Thesis Report by PiyushGoel.
[2] *"Hiding Data in Data*" in the April 2002 issue of Windows & .NET Magazine by Gary C. Kessler.
[3] A review paper titled "*Steganography and Steganalysis: Different Approaches*" by Soumyendu Das, Subhendu Das, BijoyBandyopadhyay and SugataSanyal.
[4] *"Steganography and steganalysis*" Robert Krenn, Internet Publication, March 2004 http://www.krenn.nl/univ/cry/steg/article.pdf
[5] S. Lyu and H. Farid, "*Steganalysis using color wavelet statistics and one-class support vector machines*," Proc. SPIE 5306, 35–45 - 2004.
[6] Ker, A.: *Improved detection of LSB steganography in grayscale images.* In: Proc. 6th Information Hiding Workshop. Volume 3200 of Springer LNCS. (2004) 97–115.
[7] Andrew D. Ker*," A General Framework for Structural Steganalysis of LSB Replacement*", H 2005, LNCS 3727, pp. 296–311, 2005.Springer-Verlag Berlin Heidelberg 2005.
[8] J. Fridrich, M. Goljan, R. Du, *Reliable detection of LSB steganography in grayscale and color images, Proceeding of ACM, Special Session on Multimedia Security and Watermarking*, Ottawa, Canada, 2001, pp. 27–30.
[9] Zhang, T., Ping, X.: *A new approach to reliable detection of LSB steganography in natural images. Signal Processing* 83 (2003) 2085–2093.
[10] J. Fridrich and M. Goljan, "*Practical steganalysis of digital images-state of the art*," Proc. SPIE, vol. 4675, pp. 1–13, 2002.
[11] X. Kong, T. Zhang, X. You, and D. Yang, "*A new steganalysis approach based on both complexity estimate and statistical filter*," in Proc. IEEE Pacific-Rim Conf. on Multimedia, vol. LNCS 2532, 2002, pp. 434–441.
[12] *Direct-sequence spread spectrum (DSSS), Frequency-hopping spread spectrum (FHSS)* Wikipedia, the free encyclopedia, GNU Free Documentation License http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum
[13] G.-l. Liang, S.-z. Wang, and X.-p. Zhang. *Steganography in binary image by checking data-carrying ligibility of boundary pixels*. Journal of Shanghai University (English Edition), 11(3):272–277, 2007.
[14] M. Y. Wu and J. H. Lee. *A Novel Data Embedding Method for Two-Color Facsimile Images*. International Symposium on Multimedia Information Processing, 1998.
[15] H.-K. Pan, Y.-Y. Chen, and Y.-C. Tseng. *A secure data hiding scheme for two-color images.*5th IEEE Symposium on Computers and Communications, pages 750–755, 2000.
[16] C.-C. Chang, C.-S. Tseng, and C.-C. Lin. *Hiding data in binary images*. 1st International Conference on Information Security Practice and Experience, 3439:338–349, 2005.
[17] M. Wu and B. Liu. *Data hiding in binary image for authentication and annotation*. IEEE transactions on multimedia, 6(4):528–538, 2004.
[18] Y.C. Tseng and H.-K. Pan. *Secure and invisible data hiding in 2-color images.*20th Annual Joint Conference of the IEEE Computer and Communications Societies, 2:887–896, 2001.