RANDOMIZED STEGANOGRAPHY IN SKIN TONE IMAGES

Ashita K and Smitha Vas P

Department of Computer Science & Engineering, LBS Institute of Technology for Women, Poojappura, Thiruvananthapuram

ABSTRACT

Steganography is the technique of hiding a confidential message in an ordinary message and the extraction of that secret message at its destination. Different carrier file formats can be used in steganography. Among these carrier file formats, digital images are the most popular. For this work, digital images are used. Here steganography is done on the skin portion of an image. First skin portion of an image is detected. Random pixels are selected from that detected region using a pseudo-random number generator. The bits of the secret message will be embedded on the LSB of these random pixels. An analysis is done to check the efficiency and robustness of the proposed method. The aim of this work is to show that steganography done using random pixel selection is less prone to outside attacks.

KEYWORDS

Steganography, Pixels, Pseudo-Random Number Generator, LSB, Stego Image

1. INTRODUCTION

Steganography is the method of hiding a confidential message in a common or an ordinary message and the extraction of that confidential message at its destination. The term steganography is derived from Greek which means 'covered writing' [1]. Cryptography and steganography are closely related to each other [1]. Steganography is the method of hiding the messages that it cannot be seen. Cryptography changes a message so that it cannot be understood. A secret message in the form of ciphertext might arouse suspicion while a message which is invisible or hidden created by using steganographic methods will not [1].

Steganography is mostly used on computers with digital data being the carriers and networks being the high-speed delivery channels. Different carrier file formats (text, images, audio/video etc.) can be used in order to perform steganography. In this article, digital images are used as the carrier file format. There are mainly two methods by which steganography can be performed: spatial domain steganography and transform domain steganography [2]. In spatial domain steganography, the steganography is done directly on the pixels of an image while in transform domain steganography, the image is first converted to a particular domain (cosine, wavelet, etc.) then steganography is done, after that it is converted back to its original form. This work focuses on spatial domain steganography. There are many methods in spatial domain steganography. One of the most common and popular methods is LSB. It is one of the oldest methods in spatial domain steganography. Here an encryption key is also used in LSB method. The bits of the secret message is XORed with the bits of the encryption key. Thus an encrypted message is obtained.

In this article the steganography is done on the skin portion of an image. For that, the skin region from an image is detected. The skin tone detection is done by using YCbCrcolor space. From the

DOI : 10.5121/ijcseit.2018.8301

detected skin region, random pixels are selected by using a pseudo-random number generator. The bits of the encrypted confidential message is embedded in the LSB of the random pixels. Thus a stego image is created. Then a comparison is done in order to analyze the efficiency of the proposed method based on certain parameters such as mean square error and PSNR. All programs are written by using MATLAB. In this article, there are 6 sections. Section 1. Introduction, 2.LSB method, 3.Skintone detection, 4.Randomized steganography, 5. Comparison and 6.Conclusion.

2. LSB METHOD

Least Significant Bit (LSB) based image steganography is one of the oldest steganographic methods. LSB method is the simplest scheme to hide a message in a cover image [3]. Each bit of the confidential message is placed in the LSB of the pixels of the image. Genuine receivers can extract the message from the LSB of every pixel of the original image [3]. From the pixels, only the least significant bit is altered so it cannot be visually detected by humans [3].

Here an encryption key is used. This encryption key is an integer between 0 and 255. The encryption key and the confidential message are converted to its binary format. The secret message is in its text format so it is converted to its ASCII after that it is converted to the binary format. Each bit of the encryption key is XORed with each bit of the secret message. Thus an encrypted message will be obtained. For example, if 'A' is the secret message its ASCII is 65 and its binary form is 01100101. If the encryption key is 10 its binary form is 00001010. The XOR of each bit is done. The binary form of the encrypted message is 01101111. Each bit of the encrypted message will be placed on the LSB bit of the image pixels. A stego image is thus produced.

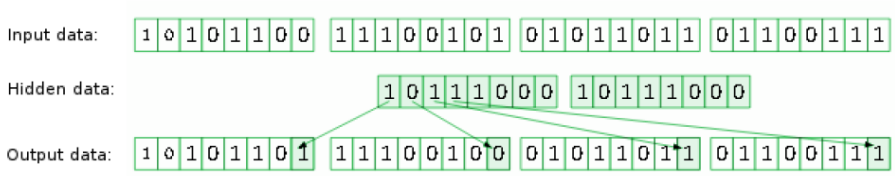

Figure 1. LSB steganography [4]

In figure 1 the input data shows the binary representation of image pixels. The hidden data shows the binary representation of the encrypted secret message. The output data shows the binary representation of the pixels of the stego image.

3. SKIN TONE DETECTION

In image steganography two types of images are used, color images and grey scale images. It is better to use color images than grey scale images because color images have large space for information hiding [5]. There are different color spaces. Some of the color spaces are RGB (Red, Green, Blue), HSV (Hue Saturation Value), YUV, YIQ, YCbCr (Luminance, Chrominance) [5].

In this paper, image steganography is done on color images. For detecting the skin region from an image YCbCr color space is used. Human eye is sensitive to changes in luminance. Any change in the chrominance is difficult to detect by the human eye. So small changes in chrominance cannot alter the image quality [5, 6, 7]. In YCbCR, Y is the luminance component, Cb and Cr are the blue and red chrominance component. The conversion formula from RGB to YCbCr is as follows [5]:

$$Y = (77/256)\,R + (150/256)\,G + (29/256)\,B$$

$$Cb = -(44/256)\,R - (87/256)\,G + (131/256)\,B + 128$$

$$Cr = (131/256)\,R - (110/256)\,G - (21/256)\,B + 128$$

The conversion formula from YCbCr to RGB is as follows [5]:

$$R = Y + 1.371\,(Cr - 128)$$

$$G = Y - 0.698\,(Cr - 128) - 0.336\,(Cb - 128)$$

$$B = Y + 1.732\,(Cb - 128)$$

The formula for detecting the skin region by using YCbCr color space is given below:

[r c v] = find (Cb <= 77 & Cb >= 127 & Cr <= 133 & Cr >=173)

By varying the values in above equation for skin tone detection, any skin tone region can be detected. Here firstly a RGB image is converted to YCbCr. From that YCbCr image the skin region is detected. Then the skin pixels are marked.

Figure 2. Original image

Figure 3. YCbCr image

Figure 4. Skin tone image

4. RANDOMIZED STEGANOGRAPHY

LSB based image steganography has disadvantages such as it is easy to decrypt if the secret key (encryption key) is known to the attacker. In order to improve the efficiency and robustness of the steganography here, the steganography is done in the randomized format. By introducing randomness it will be difficult for an attacker to find the pixels where the bits of the secret message are embedded. Even if one attacker finds those random pixels, it will be difficult for the attacker to find the correct order by which the bits of the confidential message is embedded in the pixels. This randomization of the pixels improve the efficiency and secrecy of LSB based steganography.

Two MATLAB functions are used to generate random pixels from an image. Before that, we need to find the total number of pixels available in order to perform steganography. From the detected skin region of an image, we have to select a particular skin region. The height and width of that selected region are used to find the total number of pixels. Total number of pixels in the selected region is obtained by multiplying the height and width of that selected region. MATLAB has two functions that are used to generate random numbers. The first function used is randperm (n):- this function returns a row vector containing a random permutation of the integers from 1 to n inclusive. Two or more successive calls of randperm would in most cases returns two different

values [8]. For example, first call of randperm (7) gives 5 3 6 4 7 2 1 and the second call of randperm (7) gives 4 1 7 2 3 5 6. Another function rng (seed) can be used to overcome this generation. This function helps in producing the same set of random numbers in successive calls. This function can be used at the decoder to produce a set of random numbers that is same as the set of random numbers produced at the encoder before performing steganography.

4.1. Steps

- Select the cover image and the text message.
- Then select the encryption key. A number between 0 and 255 is used as an encryption key.The encryption key and the text message are converted to its binary format.
- Now perform XOR operation. Each bit of the confidential message is XORed with each bit of the encryption key. Thus an encrypted message is obtained.
- Now find the total number of pixels available in order to perform steganography.
- Select a random seed value between 1 and 100.
- Perform the random permutation of the total number of available pixels. This will give a set of non-repeating random pixels. This is done by using aMATLAB function randperm (n). The function, rng (random seed) will produce the same set of random numbers in the correct order. This function is also used at the decoder to generate the correct sequence of random numbers obtained after random permutation. Now a sequence of random pixels are generated.
- Each bit of the encrypted message is embedded in the LSB of the random pixels generated. The embedding is done as follows:

i. $S(i,j) = C(i,j) - 1$ if $LSB(C(i,j)) = 1$ and $m = 0$

ii. $S(i,j) = C(i,j)$ if $LSB(C(i,j)) = m$

iii. $S(i,j) = C(i,j) + 1$ if $LSB(C(i,j)) = 0$ and $m = 1$

where LSB(C(i,j)) stands for LSB of cover image C(i,j) and m is the next message bit to be embedded, S(i,j) is the stego image [9].

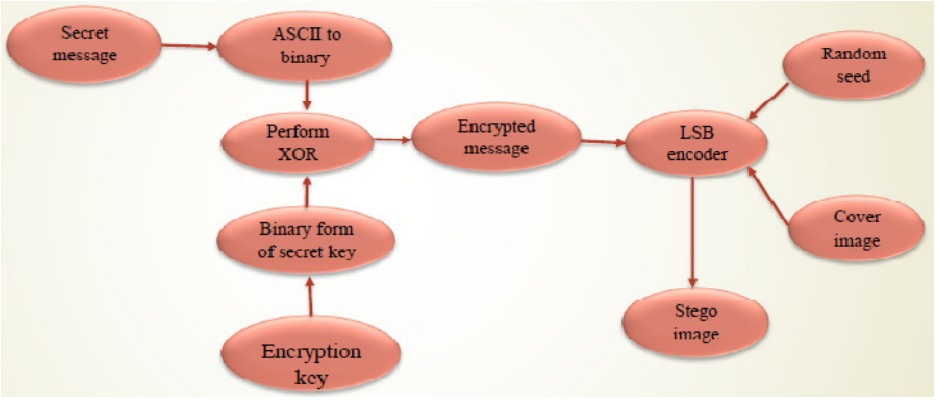

Figure 5. Flow diagram showing randomized image steganography

The result of the proposed randomized steganography is a stego image. The figure 5 shows the flow diagram of randomized steganography encryption. The decryption mechanism is the inverse of the above. The encryption key and the random seed is shared by the transmitting and receiving ends [9]. Now a comparison between the obtained stego image and the original image has to be performed to analyze the performance.

Figure 6. Original image

Figure 7. Stego image

From figure 6 and figure 7, it is obvious that human eye cannot differentiate between the original image and stego image.

5. COMPARISON

The comparison is done to analyze the performance of the proposed method. In this paper, PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) are taken as parameters for comparison. PSNR is used to evaluate the stego image quality. The formula for finding PSNR is as follows:

$$\text{PSNR} = \frac{10 \log_{10} 255^2}{MSE}$$

PSNR values below 30 dB indicate low quality (i.e., the distortion in the stego image is high) [9]. A stego image which is of high quality needs a PSNR of 40 dB, or higher [9]. MSE shows the variation between two images. It is always non-negative and it is better to have values adjacent to zero. MSE between two images g(x, y) (cover image) and g'(x,y) (stego image) is defined as

$$\text{MSE} = \frac{1}{MN} \sum_n^M \sum_m^N [g'(x,y) - g(x,y)]^2$$

where M and N are the dimensions (i.e., the width and the height) of the image.

In this paper, RGB images are considered for cover images. The secret message to be hidden is a text file. The comparison result is shown in the table below.

Table 1. PSNR and MSE values obtained for comparison.

Steganography Methods	**MSE**	**PSNR**
Ordinary LSB steganography	0.0848	58.8472
Randomized LSB steganography	0.000128	87.3362

Table 1 shows the PSNR and MSE values obtained for ordinary steganography and randomized LSB steganography. The PSNR value for randomized LSB is higher. Also, the MSE value obtained for the proposed method is closer to zero. It is obvious from the above table that the proposed method is much more secure than the ordinary LSB technique.

6. CONCLUSION

In this paper steganography is done on the skin region of an image. Here YCbCr color space is used to detect the skin portion from an image. Rather than performing ordinary LSB steganography here randomized LSB based steganography is done on the skin portion of an image. The PSNR value shows that the quality of the stego image obtained after performing the proposed method is high. Also the MSE value shows that the robustness of the proposed method is high. The efficiency of the proposed method can be checked by performing some kind of steganalysis. This can be done as a future work.

REFERENCES

[1] Neil F. Johnson &Sushil Jajodia, (2008) "Exploring Steganography: Seeing the Unseen". Computing Practices.

[2] NavneetKaur &Sunny Behal, (2014) "A Survey on Various Types of Steganography and Analysis of Hiding Techniques",International Journal of Engineering Trends and Technology, Vol. 11, No. 8.

[3] Mamta Juneja & Parvinder S.Sandhu, (2013) "An Analysis of LSB Image Steganography Techniques in Spatial Domain", International Journal of Computer Science and Electronics Engineering, Vol. 1, Issue 3.

[4] Monika Kwiatkowska and Lukasz Swierczewski, (2014) "Steganography – Coding and Intercepting the Information from Encoded Pictures in the Absence of any Initial Information", LVEE.

[5] Hemalatha S, U Dinesh Acharya & Renukka A, (2013) "Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCbCr Domains", International Journal of Advanced Information Technology, Vol. 3, No. 3.

[6] Shejul, A.A., Kulkarni, U.L., (2011) "A Secure Skin Tone Based Steganography (SSTS) using Wavelet Transform", International Journal of Computer Theory and Engineering, Vol. 3, No.1,pp.16-22.

[7] David Salomon (2004) "Data Compression–The Complete Reference", 3rd edn, Springer-Verlag,

[8] https://www.mathworks.com/help/matlab/ref/randperm.html

[9] Ramakrishna Hegde & Dr. Jagdeesha S, (2015) "Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random Encoding Technique", International Journal on Recent and Innovation Trends in Computing and Communication, Vol.3, Issue 7.

[10] Pratap Chandra Mandal Asst. Prof., Department ofComputer Application B.P.Poddar Institute of Management Technology. "Modern Steganographic technique: A Survey", International Journal of Computer Science Engineering Technology (IJCSET).

[11] Arvind Kumar Km, (2010) "Steganography- the data hiding technique", International Journal of Computer Applications (0975 – 8887) Volume 9, No.7.

[12] Niels Provos, Peter Honeyman, (2003) "Hide and Seek:An Introduction to Steganography",IEEE computer society.

[13] Deshpande Neeta, Kamalapur Snehal & DaisyJacobs, (2007) "Implementation of LSB Steganographyand Its Evaluation for Various Bits" Digital Information Management,1st International conference, pp 173-178.

[14] R.J. Andersen and F.A.P. Petitcolas, (1998) "On the Limits ofSteganography",IEEE J. Selected Areas in Comm., vol.16, no. 4, pp. 474-481.

[15] J. Fridrich, M. Goljan, and R. Du, (2001) "Distortion-FreeData Embedding", to be published in Lecture Notes in Computer Science, vol. 2137, Springer-Verlag, Berlin.

[16] Amin, Muhalim Mohamed, et al., (2003) "Information hiding using steganography",Telecommunication Technology, NCTT 2003Proceedings. 4th National Conference on. IEEE.

[17] N. Hamid, A. Yahya, R. Ahmad, and O. Al-Qershi, (2012) "Image steganographytechniques: an overview", International Journal of ComputerScience and Security (IJCSS), vol. 6, no. 3,pp. 168–187.

[18] C. Gayathri and V. Kalpana, (2013) "Study on image steganography techniques",International Journal of Engineering and Technology (IJET), vol. 5, no. 2, pp. 572–577.

[19] G. Liu, W. Liu, Y. Dai, and S. Lian, (2014) "Adaptive steganography based onblock complexity and matrix embedding", Multimedia systems, vol. 20, no. 2, pp. 227–238.

[20] R. Chandramouli, M. Kharrazi, and N. Memon, (2004) "Image steganographyand steganalysis: concepts and practice", Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 2939, pp. 35–49.

[21] J. Mielikainen, (2006) "LSB matching revisited", IEEE Signal Processing Letters, 2006, vol. 13, no. 5, pp. 285–287.

[22] B. Li, J. He, J. Huang, and Y. Shi, (2011) "A survey on image steganographyand steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142–172.

[23] M. Khodaei and K. Faez, (2012) "New adaptive steganographic method usingleast-significant-bit substitution and pixel-value differencing", IET image processing, vol. 6, no. 6, pp. 677–686.

[24] X. Li, B. Yang, D. Cheng, and T. Zeng, (2009) "A generalization of LSBmatching", IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69–72.

[25] M. Subhedar and V. Mankar, (2014) "Current status and key issues in imagesteganography: A survey", Computer Science Review, vol. 13, pp. 95–113.

[26] C. Lee and H. Chen, (2010) "A novel data hiding scheme based on modulusfunction", Journal of Systems and Software, vol. 83, no. 5, pp. 832–843.

[27] N. Akhtar, (2015) "An LSB Substitution with Bit Inversion SteganographyMethod", Smart Innovation, Systems and Technologies, Springer India, vol. 43, pp 515–521.

[28] Y. Tsai, Y. Huang, R. Lin, and C. Chan, (2016) "An Adjustable InterpolationbasedData Hiding Algorithm Based on LSB Substitution and HistogramShifting", International Journal of Digital Crime and Forensics, vol. 8, no. 2, pp. 48–61.

[29] N. Johnson, Z. Duric, and S. Jajodia, (2001) "Information hiding: steganographyand watermarking–attacks and countermeasures", Kluwer, USA.

[31] A. Cheddad, K. Condell e P. Mc Kevitt, (2010) "Digital image steganography:Survey and analysis of current methods", IEEE Signal Processing, vol.90, nº 3, pp. 727-752.

[32] T. Sharp, (2001)"An implementation of key-based digital signal steganography,in Proc. Information Hiding Workshop, vol. 2137, pp. 13-26.

[33] K. Qazanfari, R. Safabakhsh, (2014) "A new steganography method which preserves histogram: Generalization of LSB++", Information Sciences,vol 277, pp 90-101.

[34] C. Yang, F. Liu, X. Luo e Y. Zeng, (2013) "Pixel group trace model-based quantitative steganalysis for multiple least-significant bits steganography", IEEE Transactions on Forensics and Security, vol. 8, n°1, pp 216-228.

[35] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, (2000) "Hiding datain images by optimal moderately significant-bit replacement", IEE Electron. Lett. 36 (25) 20692070.

[36] Park, Y. R., Kang, H. H., Shin, S. U., Kwon, K. R. (2005), "ASteganographic Scheme in Digital Images Using Information ofNeighboring Pixels", In Proc. International Conference on Natural Computation. Berlin (Germany), Springer-Verlag LNCS, Vol. 3612, pp.962–968.

[37] Li Zhi,Sui Ai Fen., (2004) "Detection of Random LSBImage Steganography",The IEEE 2003 International Symposium on Persona1, lndoor and Mobile Radio Communication Proceedings.

[38] Shashikala Channalli &Ajay Jadhav, (2009) "Steganography an Art ofHiding Data", International Journal on Computer Science and Engineering, Vol. 1(3), 137-141.

AUTHORS

Ashita K received her B. Tech degree in Computer Science and Engineering from University of Kerala. She is now pursuing her M.Tech degree in Computer Science and Engineering from LBS Institute of Technology for Women, Thiruvananthapuram affiliated to APJ Abdul Kalam Technological University. Her areas of interest are Image Processing and Network Security.

Smitha Vas P received her B. Tech degree in Computer Engineering from Cochin University of Science & Technology, Kerala and M. Tech degree in Computer Science and Engineering from University of Kerala. Currently, she is working as an Assistant Professor in the Department of Computer Science and Engineering, LBS Institute of Technology for Women, Thiruvananthapuram affiliated to APJ Abdul Kalam Technological University. Her areas of interest are Image Processing and Machine Learning.