International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Gray Code Based Data Hiding in an Image using LSB Embedding Technique

Karthikeyan B, Asha S, Poojasree B

Abstract: ***Steganography is a mask to hide a confidential data in the form of normal text file or via audio/video. Even though there are many different types available for data hiding, our main aim is to focus on the digital image steganography because of its demand and availability, where images are in the form of pixels and can be represented in the form of binary. Since technology is developed, hackers also got developed. Therefore the security must be implemented in a better manner. To overcome the hackers, Gray code based technique is used to conceal a text in the digital image and then decrypt it. The proposed algorithm is implemented in MATLAB. This paper point is to transfer a confidential data in best and secure way where no one can recover the private information and also we can differentiate the images by using PSNR and MSE.***

Index Terms: Digital Image Steganography, Gray code, MSE, PSNR, Security, Stego image.

I. INTRODUCTION

In our day-to-day life, Message transferring and digital Communication plays an important role, especially for people who are using social Medias like Facebook, WhatsApp, Instagram, etc. Therefore for keeping the data safe and secure, steganography technology is used. In recent years, the data is transmitted over the cloud, so for the security concern steganography and cryptography are combined together to achieve the security level. Steganography overcomes all the challenges in the digital communication, and this method will not reveal the secret data or information during the process of transmission. Therefore this method provides high level security. Here the digital image is converted into binary form. Likewise message is converted into gray form. LSB substitution hides the text into the digital image by using encryption technique [11-15]. After decrypting the message, the original text will be displayed. The differences are explained by PSNR and MSE techniques. The MATLAB software is used to avoid the internet for the security concerns.

II. METHODOLOGY

This article main aim is to have a survey of Image steganography and its techniques, evaluations and how it is helpful in the future. Performance of steganography is briefly discussed in this research paper. The pros and cons of embedding system and its different types are explained. This paper overcomes the problems that are available in the existing papers. This paper moving towards the machine learning for the purpose of high quality images for the Steganography [1]. This article uses flipping images i.e., flipped the pixels not only for discrimination effects but also for the visual effects. This technique is called joint distortion measurement and this method is suitable for the secure way of transmission. This shows how we have to attach the text or message into the pixels where pixels are split up into blocks. For this method, simulator and the Visual quality are used for further understanding purpose [2]. This Steganography is based on DCT. The secret bits are hiding using LSB. Similarly low and mid frequencies are calculated by PSNR & MSE. So this will hide the secret data about the nuclear reactors into the frequencies. This tool provides more encryption with no distortion of images [3]. The Quantum Walks is the best and efficient method for designing algorithms. The novel is designed by using S-boxes (Substitution boxes). These are combined and designed in the Image steganography for the better security and data hiding. Both encryption and decryption are based on Quantum Walks. For decryption, encrypted image and the some key is enough to get a secret message. This reference paper mostly concentrates on the Visual quality and high security system [4]. This paper proposed two techniques, one is Finite Ridgelet Transform and the other one is Discrete Wavelet Transform. These both play a vital role in this modern world for its security and transmission. This technique provides more security for the color images in this developing world especially in Social Media [5]. Because of JPEG compression, while transmitting Stego image suffers a lot. To reduce this problem, researches proposed a fault-tolerant performance based on the errors and STC. This model is analyzed by the help of chi square. This method helps the coding parameter and also for data encryption integrity [6].
In this paper they discussed that video steganography is used in different ways like legal documents, copyright control. Here LSB method for developing purpose and this method used to convert all multimedia files to binary file. For this protected medium, Robustness, Embedding capacity is used. They introduced about the future popular video steganography and some challenges in the video steganography [7]. Stirling Transform main usage is in the combinatorial mathematics. This helps in integer conversion. The source sequence can be constructed by the use of (IST) Inverse Stirling Transform. The components are converted into transformed components which are related to red, green and blue channels.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Karthikeyan B*, School of Computing, SASTRA Deemed to be University, Thanjavur, India.
Asha S, School of Computing, SASTRA Deemed to be University, Thanjavur, India – Corresponding Author
Poojasree B, School of Computing, SASTRA Deemed to be University, Thanjavur, India.

This result is always zero or positive. For security purpose, the hidden data is computed constantly by the use of IST until it gets the Stego image. To verify authenticity the message digest is obtained by MD5 algorithm [8].

The paper is about various statements, measures and channels and also about security and measures in detectability. For channels solely two ways of undetectable stegosystems are available. First one is simple where the encoder knows all the facts about the stego (cipher text), but in second for encoder itself it's very difficult to understand the stego. This paper for the first time shows the relation between the work to find out the usage of steganography and distinguishing the probability of stego (hidden cipher text) distributions [9].

To solve this Steganography issues usually frequency domain is used. It has watermarking techniques (LSB + quantization techniques) to hide information within it and then Discrete wavelet Transform (Provide high robustness) (it captures both frequency and location). While decrypting the information there are some limitations. So, they introduced the Curvelet Transforms (Curvelet edges) and blind watermarking (used for watermark extraction).The important components which are mentioned in the paper are, preprocessing, Selecting Threshold, n*n, decrypt and results [10].

III. RESULT DESCRIPTION

The Flow chart diagram is shown in Fig. 1 gives the detailed structure about the image steganography. Initially, the data is placed in text (.txt) file. The text file is loaded into MATLAB and converts the text into the binary value and then binary is converted into Gray code using Bin2Gray function. To prove this, sample images in Fig. 2 (a), (c) are taken for the cover images in the image steganography. The cover images are loaded into MATLAB file; convert ASCII to the binary value. Then converted to Gray value and LSB substitution method is performed. This substitution method will remove the last two bits of each pixel value of a cover image and then replace the two bits of text gray code. The process gets repeated till the last letter of the text. For clear understanding, let's take an example. In Fig. 2 (a) cover image is embedded with 200 letters for encryption. After encrypting, stego image will display. Using stego image PSNR and MSE values are calculated. Suppose if encrypted by 1000 letters then the stego image will appear in Fig 2 (b). In all the cases, there is a difficulty in finding the difference between cover image and the stego image. So the differences are calculated by the use of PSNR and MSE values that are calculated by the use of formulae mentioned below. Some of the differences are listed in Table. 2. Finally the original data will be encrypted, decrypted and stored in the file itself.

The resultant stego images are evaluated using MATLAB software for encrypting different kinds of cover images as shown in the Fig.2. The cover image and the stego image look alike. There is a very negligible difference between the Original image and the Stego image.

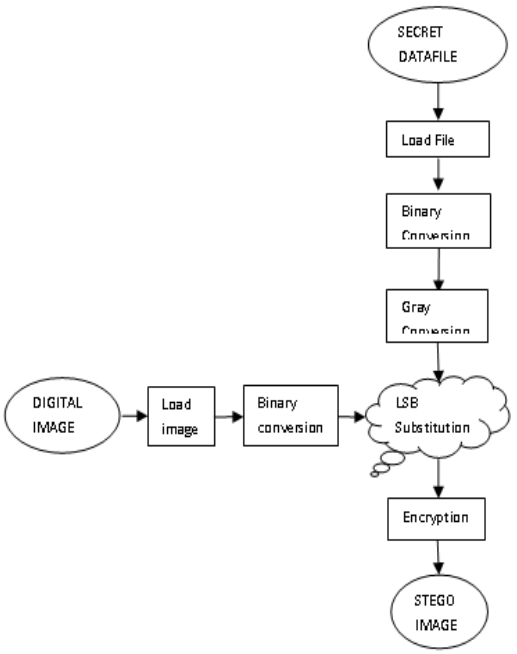

Fig. 1 Flow chart Diagram of Image Steganography

IV. MEAN SQUARE ERROR (MSE)

MSE is used to estimate the average of the squared errors. This MSE is considered to be a risk function and MSE always positive. Greater the MSE value, greater the errors. The Table 1 gives the MSE values (1),

MSE value is calculated by,

$$MSE = \frac{1}{ME}\sum_{x=1}^{M}\sum_{y=1}^{E}(I(x,y) - I'(x,y)) \quad (1)$$

Where M is the number of rows, E is the number of columns, I(x, y) is pixel value of original value.

V. PEAK-SIGNAL-TO-NOISE-RATIO (PSNR)

PSNR, Peak-Signal-to-Noise-Ratio is used to calculate the values in the form of decibels (dB). It's used to find the relationship between the maximum power of signal and the noise. Table-1 shows the difference between the cover images and the stego images. The length of the text difference is 50, 100, 200, 500, and 1000. From this, the difference between the original and stego is very negligible.

Then by using MSE, PSNR value is defined as (2),

$$PSNR = 10 * log_{10}\left(\frac{I_{max}^2}{MSE}\right) \quad (2)$$

I_{max} is the max pixel value of image.

IMAGE NAME	Text Size	MSE	PSNR
IMAGE1	50	0.000069	89.7144
	100	0.000165	85.9493
	200	0.000298	83.3858
	500	0.000777	79.2253
	1000	0.0016	76.0701
IMAGE2	50	0.000079	89.1076
	100	0.000186	85.4203
	200	0.000382	82.3045
	500	0.000901	78.5831
	1000	0.0019	75.3972
IMAGE3	50	0.000067	89.8498
	100	0.000118	87.4058
	200	0.000274	83.7452
	500	0.000625	80.1684
	1000	0.0013	77.0770
IMAGE4	50	0.000060	90.3405
	100	0.000140	86.6442
	200	0.000275	83.7368
	500	0.000291	79.5025
	1000	0.0015	76.3099
IMAGE5	50	0.000050	91.0806
	100	0.000111	87.6629
	200	0.000217	84.7617
	500	0.000566	80.5989
	1000	0.0011	77.6131

Table. 1 Differences between cover and stego images in PSNR and MSE

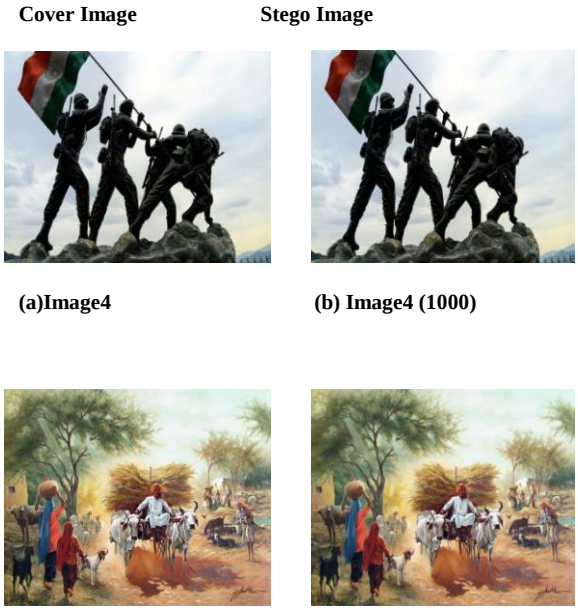

Fig. 2 Different kinds of cover and stego images

VI. CONCLUSION

In the developing countries, technologies are growing very quickly but Privacy and Security is reduced. So to increase the security and to hide the message/confidential data from the illegal users or hackers this paper is proposed. This paper talks more about the algorithms related to the binary and gray code in terms of the digital image. Where the text file is attached and converted into the gray code and hide it in the digital image and then decrypt it. This entire work is done by the use of Matlab Software, so there is no need of network communication system. The differences between the original and the Stego images are distinguished with the help of PSNR and MSE values for our clear understanding. From the analysis, this paper concludes that no one can disclose the confidential data.

ACKNOWLEDGEMENT

Authors would like to convey their thanks to SASTRA deemed to be University for providing infrastructure facility to do this paper work.

REFERENCES

1. Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial, Brendan Halloran "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research", Neurocomputing, Volume 335, 28 March 2019, Pages 299-326
2. Junhong Zhang, Wei Lu, Xiaolin Yin, Wanteng Liu, Yuileong Yeung "Binary image steganography based on joint distortion measurement", Journal of Visual Communication and Image Representation, Volume 58, January 2019, Pages 600-605
3. Sahar A.El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information", Computers & Electrical Engineering, Volume 70, August 2018, Pages 380-399.
4. Ahmed A. Abd EL-Latif, Bassem Abd-EI-Atty, Salvador E. Venegas-Andraca "A novel image steganography technique based on quantum substitution boxes", Optics & Laser Technology, Volume 116, August 2019, Pages 92-102
5. Rohit Thanki, Surekha Borra "A color image steganography in hybrid FRT–DWT domain", Procedia Computer Science, Volume 79, 2016, Pages 321-327, open access
6. Yi Zhang, Xiangyang Luo, "On the fault-tolerant performance for a class of robust image steganography", Signal Processing, Volume 146, May 2018, Pages 99-111
7. Liu, Yunxia, Liu Shuyang, Wang, Yonghao, Zhao, Hongguo, Liu, Si "Video steganography: A review", Neurocomputing, Volume 335, 28 March 2019, Pages 238-250
8. S.K.Ghosal, J.k.Mandal, "On the use of the stirling Transform in image steganography", Journal of Information Security and Applications, Available online 22 April 2018, in press, Corrected Proof.
9. Maciej Liskiewicz, Rudiger Reischuk, Ulrich Wolfel, "Security levels in steganography – Insecurity does not imply detectability", Theoretical Computer Science, Volume 692, 5 September 2017, Pages 25-45.
10. S. Edward Jero, Palaniappan Ramu, S.Ramakrishnan, "ECG steganography using curvelet transform", Biomedical Signal Processing and Control, Volume 22, September 2015, Pages 161-169.
11. Charan GS, NithinKumar SSV, Vaithiyanathan V, Divya Lakshmi, Karthikeyan B "A novel LSB based image steganography with multi-level encryption", ICIIECS 2014-2015, IEEE International Conference on Innovations in Information, Embedded and Communica-tion Systems, 12 August 2015, Article number 7192867.
12. Nithin Kumar SSV, Charan GS, Karthikeyan B, Vaithiyanathan V, Rajasekhar Reddy M, "A hybrid approach for data hiding through chaos theory and reversible integer mapping", International Conference on Computational Intelligence, Cyber Security and Computational Models, ICC3 2015; Coimbatore; India, Volume 412, 2016, Pages 483-492.
13. B Karthikeyan., Shaik Zunaid Sameer., P Srinath., Anishin Raj M M., V.Vaithiyanathan., "A Novel Stretching Approach For Multiple Image Steganography Using Bit Stuffing", In-ternational conference on Communication & Security, 2017.
14. Sriram S, Karthikeyan B, Vaithiyanathan V, Raj MMA, "An approach of cryptography and steganography using rotor cipher for secure transmission"2015 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2015, 17 March 2016, Article number 7435669.

15. Karthikeyan B, Ramakrishnan S, Vaithiyanathan V, Sruti S, Gomathymeenakshi M, “An improved steganographic technique using LSB replacement on a scanned path image”, International Journal of Network Security, Volume 16, Issue 1, January 2014, Pages 14-18.

AUTHORS PROFILE

Karthikeyan B completed his Ph.D in Computer Science & Engineering from SASTRA Deemed to be University, Thanjavur in 2015. He has published more than 40research papers in SCOPUS indexed journals and conferences. His area of interest is Image Compression, Steganography and Machine learning.

Asha S She is studying B. Tech Information Technology in SASTRA Deemed to be University, Thanjavur. She has published IEEE conference paper in the field of Steganography and Cryptography. She was very interested to study about Data hiding and Data Security in the field of Steganography. Her area of interest is Steganography, Cryptography and Computer Networks.

Poojasree B She is studying B.Tech Information Technology in SASTRA Deemed to be University, Thanjavur. She has published IEEE conference paper in the field of Steganography and Cryptography. She was curious about Data Security and Data Protection. Her area of interest is Steganography, Cryptography and Design analysis and algorithms.