ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse148932020.pdf
https://doi.org/10.30534/ijatcse/2020/148932020

An Improved Method for LSB Based Image Steganography Technique using Collatz Conjecture Sequence

Karthikeyan B[1], Gokul K[2], Balasubramanian K[3]andAnishin RajM.M[4]
School of Computing, SASTRA Deemed to Be University, Thanjavur-613401, India, mbalakarthi@gmail.com[1]
School of Computing, SASTRA Deemed to Be University, Thanjavur-613401, India, gokulk404@gmail.com[2]
School of Computing, SASTRA Deemed to Be University, Thanjavur-613401, India,viratbala10@gmail.com[3]
Department of CSE, Viswajyothi College of Engineering and Technology, Vazhakulam - 686670, India, anishinraj@gmail.com[4]

ABSTRACT

Insecure data is one among the biggest threats nowadays. Hence, there are many techniques for securing and transmitting such secret data. One such technique is called steganography. Steganography is a technique of hiding a secret data in digital media which include images, videos and audio. Among the various media available, this paper focuses to implement image steganography. In this paper, Collatz Conjecture function is used that returns the index values in which the secret data is hidden. Collatz Conjecture is a function which takes one positive integer argument n and returns 3n+1 if the argument received is odd else, it returns n/2. In general, to provide security to data in communication, cryptographic methods are used to convert ordinary data to some other form using the key but it is not as secure as image steganography, because, in this, secret messages are split and stored in various indices on the image pixels.

Key words: Collatzconjecture, image steganography, security, secret data.

1.INTRODUCTION

The ultimate aim of image steganography is to hide a message inside a digital image. Earlier, for secured communication, symmetric key cryptography, asymmetric key cryptography and various other methods were used to encrypt a secret message into an unknown message which had no form. But it wasn't sure that the message was securely transmitted because in case the intruder somehow finds the key, the secret message could be cracked easily. So, if the secret message is split into small units and if the small units are stored in various indices (pixels) of an image , even if the intruder finds the key, only the first small unit of secret message could be cracked and it would be impossible to crack the entire secret message as the intruder doesn't know the respective indices of the next small units of the secret message.

Collatz Conjecture function enhances the un-detectability of the secret message which works based on the index value that is returned by the collatz conjecture function, the respective ASCII bits of the secret data is encoded in the image file as discussed in [1],insecurity doesn't imply the detectability but there is chances where the intruder can include his own message into the image by using that in security. so the collatz conjecture sequence also helps us to prevent that problem by providing additional security to the message.

The integer value "n" given for the collatz conjecture function is used as a key for both encoding and decoding in image steganography. That is, "n" is the starting index from where the respective ASCII bits of secret message have been encoded in the image on the sender side and the same is used to extract the secret message from the image on the receiver side.

2.LITERATURE SURVEY

Maciej et.al. discusses various security notations used in steganography and also proposes different variants of undetectability and security levels of a steganosystem [1].

Karthikeyan, et al. were made some experiments and discussions on image steganography by using enhanced hill cipher cryptography approach to encrypt the image in the method they used [2][16].

Inas Jawad Kadhim et.al. Proposed edge-based image steganography which provides higher payload capacity using various machine learning techniques and they also approaches a process which enables adaptive embedding of

sub-band coefficients of Dual Tree Complex Wavelet Transform (DT-CWT) [3].

Ying Zou et.al. proposed steganalysis for multi-class steganography, which explains a method that captures statistical characteristics by various deep learning methods and provides low embedding rate .The ultimate aim of their proposal is Construction of steganalysis detectors that doesn't distinguish steganalysis algorithms of any specific type [4].

Xinyi Zhou et.al. proposed a secure way to hide secret colour image inside another image by combining and using RSA algorithm of cryptography and LSB algorithm of image steganography [5].

Hemalatha et.al. proposed a strategy to hide the audio signals inside the image using steganography method. They used the wavelet transform method to transform any audio format and hide the resulting signal inside an image [6].

Rupali Bhardwaj et.al. proposed an image steganography method which provides security in three levels[17]. The secret message is first complemented, then it is hid in a digital image using random number generator and finally to improve the security, the inverted LSB method is used[7].

Mansi et.al. provided the survey which focuses on elementary concepts, estimation, measures and security aspects of image steganography system and they also discuss issues in image quality metrics and several spatial and transform domain embedding schemes [8].

Zeyad Safaa Younus et.al. proposed an image steganography technique which uses Vigenere Cipher and Huffman Coding methods to encrypt and compress the secret message inside the cover image. By using this method they combined cryptography and steganography to increase the efficiency and robustness [9].

Mamta Jain et.al. proposed an image steganography method which uses dynamic/adaptive circular queue Least Significant Bits (LSBs) substitution[15] and RSA cryptosystem to maintain confidentiality, integrity and to encode and decode secret data inside the cover image [10].

S.K. Sabnis et.al. proposed a steganalysis of high capacity image steganography method which is based encryption by wavelet-based fusion that uses image quality metrics (a set of features) and they also compared their steganography techniques with two different encryption methods on an undetectable basis [11].

Karthikeyan, et al. were made some experiments and discussions on image steganography method which includes combined approach of Least Significant Bits (LSBs) encoding Steganography[14] technique and algorithm that implements Data Encryption Systems (DES) [13].

3.RESULTS AND DISCUSSION

In the following section, some experiments are carried out to check the efficiency of the proposed image steganography technique. The general explanation is as follows:

3.1.On the Sender Side

The input for the software is the secret message and thekey. The key is nothing but the input for the collatz conjecture function. Based on the key value, the collatz conjecture function will recursively return the indices values.

Then the secret message is converted into its respective ASCII bits. Each pixel of the image will have Red-Green-Blue (RGB) values of 8 binary bits each.

Each character of the secret message is processed and converted to its respective ASCII value of size 8-bits. If ASCII value is less than 8-bits then 0's are padded at the front to generate an 8-bit binary value.

Then ASCII bits of the secret message are spliced into small chunks of binary bits of size 2 each.Based on the index value returned by the Collatz Conjecture function, the chunk of size 2 binary bits will be encoded into the least 2 significant binary bits of blue value of the respective pixel.

The process will continue till all the chunks (binary bits of size 2 each) of secret message are encoded into the indices/pixels (returned by collatz conjecture function) of the cover image Finally, the steganoimage is created.

3.2. On the Receiver Side

The input for the software is the key. The key is nothing but the input for the Collatz Conjecture function. Based on the key value the Collatz Conjecture function will recursively return the indices' values.

Each pixels of the image will have Red-Green-Blue (RGB) values of 8 binary bits each, based on the index value returned by the Collatz Conjecture function. The respective index/pixel of the steganoimage is processed and the least 2 significant binary bits of blue value will be decoded, copied and appended into the temporary variable.

The process of appending least 2 significant binary bits of blue value will continue until all the indices (returned by collatz conjecture function) are processed. Then the value of temporary variable is reversed and is converted to its respective ASCII value by treating 8 binary bits as one character. Finally, the secret message will be displayed.

3.3. Implementation of Collatz Conjecture

CollatzConjecture(n)

1. If n == 1
2. return
3. else if n is odd
4. CollatzConjecture((3*n)+1)
5. return
6. else
7. CollatzConjecture(n/2)
8. Return

3.4. Working of Proposed Method

In sender side, the workflow of proposed method is explained below and is depicted by the flowchart shown in Figure 1.

Read the cover image onto which the secret message is to be encoded.

Read the secret message and read the key. (Common for both sender and receiver)

Convert the message to its respective ASCII bits.

Run the Collatz Conjecture function by passing the key as a parameter.

Encode the secret message to the pixels of the cover image which is returned by the Collatz conjecture function and hence final steganoimage will be generated.

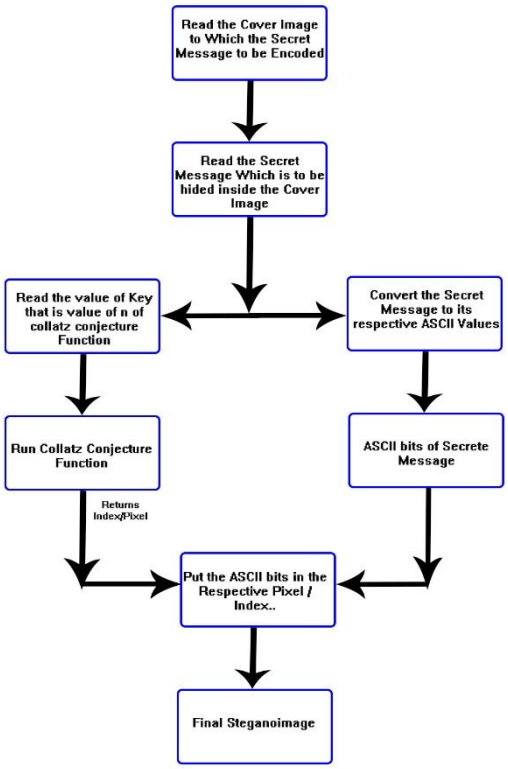

Figure 1: Flowchart of proposed Method in Sender Side

In receiver side, the workflow of proposed method on is explained below and is depicted by the flowchart shown in Figure 2.

Read the received cover image and read the key. (common for both sender and receiver)

Run the Collatz Conjecture function by passing the key as a parameter.

Process the index/pixel (returned by the Collatz Conjecture function) of the cover image and decode the secret message.

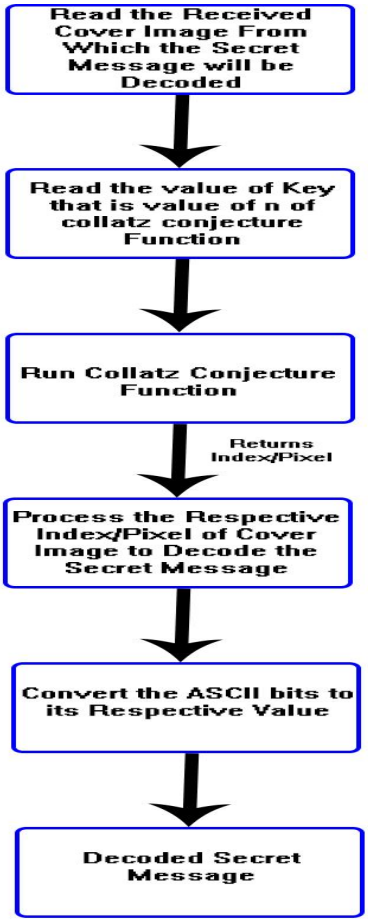

Figure 2: Flowchart of proposed Method in Receiver Side

3.5. Sample Images

Cover image before encoding the secret message (PNG format (first two pictures from left) and BMP format(last picture from left)) are shown in Figure 3.

Figure 3: Cover Images used for testing(before encoding the data)

After encoding the secret message "SeCuRiTy" with the key 50, the resultant cover images (PNG format (first two pictures from left) and BMP format (last picture from left)) are shown in Figure 4.

Figure 4: Cover Images used for testing (after encoding the data)

3.6. Formulas Used

The difference between steganoimage and the normal image can be found using the following formulas.[12]

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where,

m, n=Number of rows and columns, I (I, j) =Pixel value before encoding the data (I, j) =Pixel value after encoding the data.

$$PSNR = 10\,log\frac{(255)^2}{MSE}$$

Where,

MSE=Mean Square Error value of the input image

3.7.Tabulation

We have experimented the method with various values using various formats of images and is tabulated in Table 1,

Table 1: Results of Experiment

No	Secret Message	Image Size	Image Format	MSE Value	PSNR Value
1	"SECURE"	950*1000	PNG	0.0001342	86.94379
2	"SECURE"	950*1000	BMP	0.0017750	75.63865
3	"Key=19"	950*1000	PNG	0.0000609	90.27815
4	"Key=19"	950*1000	BMP	0.0017046	75.81456

4. CONCLUSION

The ultimate aim of every steganography technique is to secure the secret message inside an image without affecting the quality of the respective image, but the drawback is that in most of the steganography methods, security of the secret message depends only on the key used, which means if the key is harder to crack, then it implies that the secret message is more secure, else, it implies that the secret message is less secure. In our method, we provide additional security to the secret message by using a function Collatz Conjecture. Hence even if the key is less secure, the secret message has additional security. The Collatz Conjecture function also doesn't affect the image quality as the Mean Squared Error (MSE) value is less which implies high Peak Signal to Noise Ratio (PSNR) value which is an important aspect of image quality.

REFERENCES

[1] Maciej Liśkiewicz,Rüdiger Reischuk,and Ulrich Wölfel,**Security levels in steganography – Insecurity does not imply detectability**, Theoretical Computer Science, 692, 25-45, 2017. https://doi.org/10.1016/j.tcs.2017.06.007

[2] Karthikeyan, B, Chakravarthy, J, and Vaithiyanathan, V,**An enhanced Hill cipher approach for image encryption in steganography**, 2013 International Journal of Electronic Security and Digital Forensics 5(3-4), pp. 178-187,2013. https://doi.org/10.1504/IJESDF.2013.058652

[3] Inas Jawad Kadhim,Prashan Premaratne,and Peter James Vial, **High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform**, Cognitive Systems Research, 60, 20-32, 2019. https://doi.org/10.1016/j.cogsys.2019.11.002

[4] Ying Zou, Ge Zhang, and Leian Liu,**Research on image steganography analysis based on deep learning**, Journal of Visual Communication and Image Representation, 60, 266-275, 2019. https://doi.org/10.1016/j.jvcir.2019.02.034

[5] Xinyi Zhou, Wei Gong, WenLong Fu, and LianJing Jin, **An improved method for LSB based color image steganography combined with cryptography**, International Conference on Computer and Information Science (ICIS),1,1-4,2016. https://doi.org/10.1109/ICIS.2016.7550955

[6] HemalathaS, DineshAcharyaU, and RenukaA, **WaveletTransform based steganography technique to hide audio signals in image**, Procedia Computer Science,47,272-281,2015.

[7] Rupali Bhardwaj, and Vaishali Sharma,**Image steganography based on complemented message and inverted bit LSB substitution**,Procedia Computer Science,93,832-838,2016.

[8] Mansi S. Subhedar, and Vijay H. Mankar, **Current status and key issues in image steganography: A survey**, Computer Science Review,13-14, 95-113,2014.

[9] Younus.Z.S, and Hussain.M.K, **Image steganography using exploiting modification direction for compressed encrypted data**, Journal of King Saud University–Computer and Information Sciences,https://doi.org/10.1016/j.jksuci.2019.04.008.

[10] Mamta Jaina, Saroj Kumar Lenkab, and Sunil Kumar Vasistha, **Adaptive circular queue image steganography with RSA cryptosystem**, Perspectives in Science,8,417-420,2016.

[11] Sabonis S.K, andAwakeR.N, **Statistical steganalysis of high capacity image steganography with cryptography,** Procedia Computer Science, 79, 321 – 327,2016.

[12] Rafael C. Gonzalez,and Richard E. Woods. Digital image processing, ed. 2, Pearson Education,2012.

[13] Karthikeyan B, Deepak A, Subalakshmi K.S, Anishin RajM.M, and Vaithiyanathan V, **A combined approach of steganography with LSB encoding technique and des algorithm**, 2017 Proceedings of the 3rd IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB7972388, pp. 85-88, 2017.

[14] Sriram S, Karthikeyan B, Vaithiyanathan V, and Raj M.M.A. **An approach of cryptography and steganography using rotor cipher for secure transmission,** IEEE International Conference on Computational Intelligence and Computing Research, ICCIC, 2015.

[15] Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, and Rushdi Abu zneit. **Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography**, International Journal of Advanced Trends in Computer Science and Engineering, vol 8, No.3, May - June 2019. https://doi.org/10.30534/ijatcse/2019/64832019

[16] Gomathymeenakshi M, Sruti S, Karthikeyan B, and Nayana M. **An efficient arithmetic coding data compression with steganography**, 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, ICE-CCN, pp. 342-345,2013.

[17] Marilou O. Espina, Arnel C. Fajardo, Bobby D. Gerardo, and Ruji P. Medina. **Multiple Level Information Security Using Image Steganography and Authentication**, International Journal of Advanced Trends in Computer Science and Engineering, Vol 8, No.6, November – December 2019. https://doi.org/10.30534/ijatcse/2019/100862019