Knight Tour for Image Steganography Technique

Manjot kaur Bhatia

***Abstract:** The growth rate of the Internet is exceeding that of any previous technology. As the Internet has become the major medium for transferring sensitive information, the security of the transferred message has now become the utmost priority. To ensure the security of the transmitted data, Image steganography has emerged out as an eminent tool of information hiding. The frequency of availability of image file is high and provides high capacity. In this paper, a method of secure data hiding in image is proposed that uses knight tour positions and further 8-queen positions in 8*8 pixel blocks.The cover image is divided into 8*8 pixel blocks and pixels are selected from each block corresponding to the positions of Knight in 8*8 chessboard starting from different pixel positions. 8-pixel values are selected from alternate knight position. Selected pixels values converted to 8-bit ASCII code and result in 8* 8 bit matrix. 8-Queen's solution on 8*8 chessboard is applied on 8*8 bit matrix. The bits selected from 8-Queens positions and compared with 8-bit ASCII code of message characters. The proposed algorithm changes the LSB of only some of the pixels based on the above comparison. Based on parameters like PSNR and MSE the efficiency of the method is checked after implementation. Then the comparison done with some already proposed techniques. This is how, image steganography showed interesting and promising results when compared with other techniques.*

***Keywords:** Information hiding, Image steganography, Security, secure message communication, secret message, 8-Queen's, Knight tour*

I. INTRODUCTION

The Internet has been growing at unprecedented rates and has emerged as the most convenient and efficient medium of communication. Fast and cheap transfer can be done through internet in various fields like private sector, government offices, medical areas and military. The confidentiality of the transferred message needs to be preserved. An appropriate method is needed to ensure that the message is transferred securely and safely over the network. Steganography proves to be a trustable technique for achieving this aim. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., audio files, video files and images. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. The word steganography is made up of two words of ancient Greek origin "steganos" meaning covered, concealed or protected and "graphic" meaning writing. *Steganographic* techniques have been used date back to ancient Greece around 440BC, Herodotus sent secret messages using this concept. Greeks also wrote message on wood covered with ink. Invisible ink concept was also used during the period of World War II. According to Greek history, bald scalp of the slaves were used to write secret messages, and after the growth of hair, they were sent as messengers. Steganography is an art and science of secret communication used to hide secret information within a cover media like image, audio and video files in such a way that prevents an unauthorized user to detect hidden message [Medeni,2010]. Image files are very much in use now a day due to their high capacity and easy availability over the internet. At the sender's site, the image used for embedding the secret message referred as cover image, and the secret information that needs to protect is termed as a message. The embedding algorithm used to hide message in cover image, resulting stego image that transferred to the receiver and receiver extracts out the secret message using extraction algorithm. Cryptography technique also used for secure transmission of messages over the internet but steganography is becoming more popular because of its advantages over cryptography. Cryptography hides the exact meaning of message from the third party whereas steganography hides the very existence of the message itself.

II. LITERATURE REVIEW

In recent years, steganography has emerged as one of the main research areas in information security. Here, we will discuss some already proposed methods, and the comparison between the already proposed methods.

A number of data embedding techniques based on the method of replacing the least-significant bits (LSBs) of the pixels of the cover image. LSB method provides the very basic idea of image coding. It states that the secret message bits can be placed by replacing the least significant bits of the pixels of the image. 100% insertion of message binary bits is allowed in the pixels of an image with a very minute change of +1 or -1 in the value of the pixels. The disadvantage of this method was that it was vulnerable to attack as the intruder can access the data by only picking the LSB's because message was present at LSB. Intruder can easily decode this method and also it is not immune to noise and compression techniques. There are various other methods for data hiding such as pixel-value difference methods, histogram modification and pixel mapping methods using spatial domain. Many researchers have worked in this area and proposed or developed many image information hiding methods [Cole, 2003;Petitcolas,1999; Sullivan,2004;Warkentin,2008;Emam,2007;Kumar,2010; Bhatia,2013,2015]. Bhatia in 2014 proposed image steganography using spread spectrum approach. Spread spectrum approach uses the properties of orthogonal image planes and spread the modulated message in one image plane of cover image. Using this method, secret message can be extracted from the stego image without the cover image.Another method was proposed by Singh et al., 2005 which is based on 1st and 2nd bit plane.

Retrieval Number: F8736088619/2019©BEIESP
DOI: 10.35940/ijeat.F8736.109119

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The message was hidden according to the combination of 1st and 2nd bit plane. The conclusion was that the probability of message insertion at a pseudorandom location at first was 50% when there was no need to change the pixel value and 12.5% when a change in pixel was required. Batra and Rishi, 2010 proposed a method in which the message was hidden using the 6th, 7th and 8th bits of a pixel in a grayscale image and it overcomes the limitation of the Singh et al's method. The main conclusion of the method was probability of message insertion at a pseudorandom location was 85.93% and 43.18% when the message was not changed. So this method does not provide 100% message insertion rate. FMM (Five Modulus method) had a different perspective. In this method, the cover image was divided into N blocks with block size k*k pixels where k is the size of the window. To make the pixel divide by 5, each pixel in the block modified. And thus, the message was scattered all over the image. Low hiding capacity was the major limitation of this method. The facts of the Stego Color Cycle(SCC) method presented by Bailey and Curran, 2006 is the advanced version of the LSB method. In this also, the LSB of pixels of color images are used for insertion of secret message binary bits but here insertion is done in a cyclic way. It works by choosing the LSB of the red channel of first pixel and then LSB of the green channel of second pixel and then LSB of the blue channel of third pixel, and then the cycle is repeated in the same cyclic order for all pixels. 100% insertion for RGB images is seen here but for its simple cyclic order, the intruder can easily decode it. To remove the fallacies of this method some more techniques were introduced. Gutub, 2010, presented the pixel indicator method. It is applied to RGB images in which two channels of the image are used for storing the data based on the value of the third channel that acts as an indicator channel. Bhatia, 2017 proposed a message hiding technique that uses three image planes RGB of the cover image Each image plane is further divided into 8*8 pixels blocks and uses the positions of 8-rooks on 8*8 chessboard for hiding message characters.

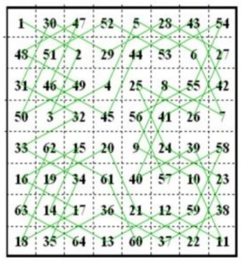
A. Knight tour in a chessboard

Knight tour is a continuous move of knight on a chessboard in such a way that it visits every square only once. If the knight moves end in the same square from which it started then is called closed tour else it is open tour. The knight tour problem is the mathematical problem and first mathematician to solve this problem was Leonhard Euler. In 1823 H. C. von Warnsdorf. Schwenk described the method Warnsdorf's rule used to complete the Knight Tour. The number of all directed tours (open and closed) on an $n \times n$ board for $n = 1, 2, \ldots$ are(wikipedia, 19th June, 2019):

1; 0; 0; 0; 1,728; 6,637,920; 165,575,218,320; 19,591,828,170,979,904.

The number of all directed tours (open and closed) on an n × n board for n = 1, 2, … are:

1; 0; 0; 0; 1,728; 6,637,920; 165,575,218,320; 19,591,828,170,979,904. (sequence A165134 in the On-Line Encyclopedia of Integer Sequences).



1	30	47	52	5	28	43	54
48	51	2	29	44	53	6	27
31	46	49	4	25	8	55	42
50	3	32	45	56	41	26	7
33	62	15	20	9	24	39	58
16	19	34	61	40	57	10	23
63	14	17	36	21	12	59	38
18	35	64	13	60	37	22	11

Figure 1: Some of the possible Knight Tour

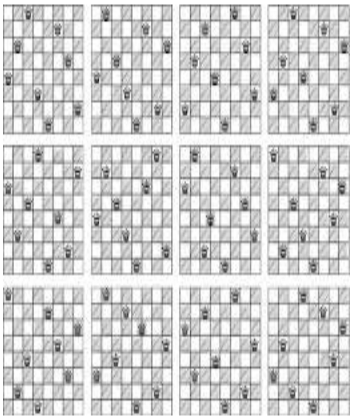


Figure 2: Some of the possible 8-Queens solutions

In this paper, we have proposed a message hiding technique using solutions of Knight tour and placing 8-Queen's problem in an 8*8 chessboard. The proposed technique divides the cover image into 8*8 pixels blocks. Knight tour is applied to each 8*8 pixel block. The proposed method selects pixels from the alternate knight's position. The selected 8-pixels are expanded to 8*8 Ascii bit matrix._8-Queen's solution applied to 8*8 bit matrix excluding the last column of the matrix. The collected 7-bits are compared with 7-bit Ascii code of the message characters. Last column bit of 8*8 bit matrix is set '0' or '1' depending upon result of bit comparison. The cover image and stego image can be compared using Peak Signal to Noise ratio(PSNR). The paper organized in four sections. Section 2 discusses Literature review. In section 3, we present the basics of steps used in proposed image steganography method. The proposed embedding and extraction algorithms are presented in the section 4. The paper concluded in the last section.

III. PROPOSED IMAGE STEGANOGRAPHY TECHNIQUE

The objective of our research is to propose an image steganography technique that hides secret data in an image in a way that it needs to do slight modifications in the cover image. The proposed technique divides the cover image into 8*8 pixels blocks. Each pixel block of image is considered as a 8*8 chessboard. The proposed algorithm applies knight moves and stego key on each 8*8 pixels block. The knight tour moves on a chessboard in such a way that it visits every square only once i.e. here as 8*8 pixel block considered as chessboard so knight moves on all the 64 pixels in the block.

Proposed method selects the 8-pixels from the alternate positions of the knight tour and converts the selected 8-pixels into 8-bit ASCII code resulting into 8*8 bit matrix. The message characters converted into 7-bit ASCII code.

In our proposed algorithm, we are also using the solution set for the problem of placing 8-non-attacking Queens in an 8*8 chessboard. The algorithm compares the bits from 8*8 bit matrix of the pixels, located at the positions corresponding to the placement of Queen's in the first 7 columns of the 8*8 chessboard with 7-bits(ASCII code) of the message character. If the bit matches, proposed algorithm sets the 8th column bit as '0' otherwise it sets 8th column bit as '1' of the 8*8 bit matrix of the image block. When all the message characters embedded into the blocks of cover image, stego image is generated Figure 3 shows the diagram for the proposed message hiding technique.

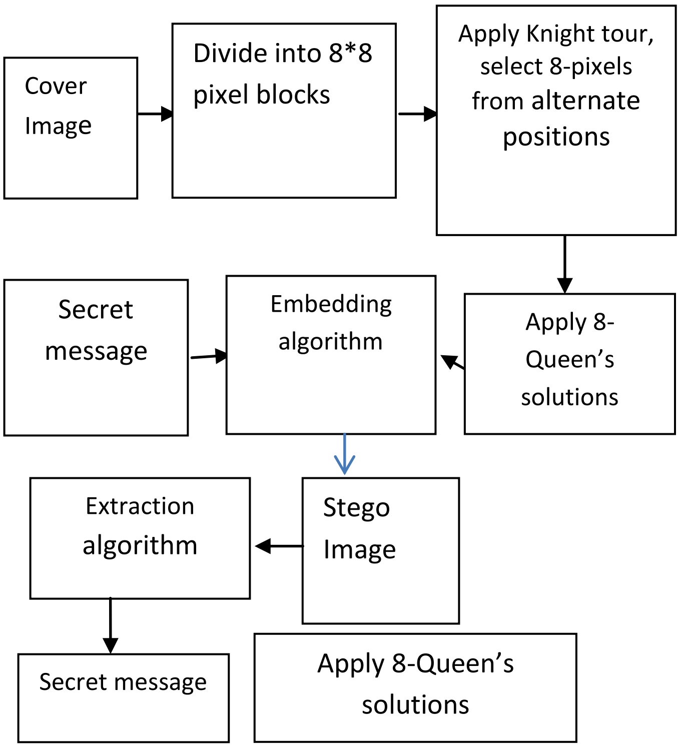

Cover Image
Divide into 8*8 pixel blocks
Apply Knight tour, select 8-pixels from alternate positions
Secret message
Embedding algorithm
Apply 8-Queen's solutions
Extraction algorithm
Stego Image
Secret message
Apply 8-Queen's solutions

Figure 3 Sequence of operations in the proposed method

IV. PROPOSED EMBEDDING AND EXTRACTION ALGORITHM

A. Embedding algorithm

The proposed algorithm divides the cover image into 8*8 pixel segments. The different solutions of Knight Tour starting from different positions in 8*8 chessboards, need to be saved. The different moves of knight tour shown in Figure 1. The embedding algorithm stores the different solutions of placing 8-Queens in an 8*8 chessboard, some of the possible solutions are shown in Figure 2. The proposed embedding algorithm selects the starting position of knight in 8*8 pixel block by finding soft dipole value of that pixel block, called stego key.

i.e. first position of knight= soft dipole value of 8*8 image block,

Now, select 8-pixels from the alternate positions of the 64 Knight tour moves in the image block. Expand the above selected 8 pixels values (in byte) into 8 bit ASCII code resulting into 8*8 bit matrix. Apply 8-queen's solution to the 8*8 bit matrix and collect the 7-bits from the 7 positions of queen excluding bit at the last column position of queen. Save it in an array Q[].Convert the message character into 7-bit ASCII code and save in two-dimensional array m[i,7]. Compare each bit of 7-bits saved in an array Q[] with bit at the corresponding position from 7-bits of ith message character m[i,7]. If two bits are same, mark last column bit of that row as '0' otherwise mark last column bit as '1'.

B. Extraction algorithm

The extraction algorithm divides each image into 8*8 pixels blocks. Knight tour is applied to each block. The extraction algorithm selects 8 pixels from the alternate positions of the positions visited by knight tour. The selected 8 pixels are converted to 8-bit ASCII code resulting 8*8 bit matrix. Proposed algorithm applies 8-Queen's solution to 8*8 bit matrix and selects 7 bits corresponding to queen's position excluding last column. If the last column bit at the row corresponding to queen's position is '0' , save the bit at the queen's position but the last column bit at the row corresponding to queen's position is '1', then flip the bit at queen's position and save the flipped bit. The extracted 7-bit represents one message character. Each 8*8 pixel block extract one message character.

V. EXPERIMENTAL RESULTS

Experiments will be conducted on the images with different formats like BMP, PNG and JPG. To evaluate the performance of the proposed algorithm, Peak-Signal-to-Noise ratio (PSNR) is used to measure the quality of the stego image, which is defined in equation 1, for an M × N gray scale image.

$$\text{PSNR}=10 * \log 10 \frac{255^2 * M * N}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(p_{i,j}-q_{i,j}\right)^2} \text{ dB} \qquad (1)$$

Where $p_{i,j}$ and $q_{i,j}$ represent the cover image pixels and stego image pixels. *M* and *N* represent height and width respectively of the images. Histogram of images is also used to compare the cover image and stego image.

VI. CONCLUSION

The proposed algorithm can be used for secure group communication and secure message transmission between the intended receivers. The algorithm increases the embedding capacity by using the all the 8*8 pixel blocks of the cover image for hiding message. Proposed embedding method provides two level securities by using knight tour and 8-Queen's solution in 8*8 pixel block. The proposed method is secure as an attacker requires stego keys to extract hidden information. In future, the proposed method will be applied on images of different formats: BMP, JPG and PNG. Experimental results will be presented to give better security for secure group communication.

REFERENCES

1. S. Batra and R. Rishi, "Insertion of message in 6th, 7th and 8th bit of pixel values and its retrieval in case intruder changes the least significant bit of image pixels," *International Journal of Security and Its Applications*, vol. 4, no. 3, pp. 1–10, 2010.
2. P. Singh, S. Batra, and H. R. Sharma, "Evaluating the performance of message hidden in first and second bit plane,"

WSEAS Transaction on Information Science and Technology, vol. 2, no. 8, pp. 1220–1222, 2005.

3. K. Bailey and K. Curran, "An evaluation of image based steganography methods," *Multimedia Tools and Applications*, vol. 30, no. 1, pp. 55–88, 2006.
4. A. A.-A. Gutub, "Pixel indicator technique for RGB image steganography," *Journal of Emerging Technologies in Web Intelligence*, vol. 2, no. 1, 2010.
5. Bhatia, M. K., "8-Rooks Solutions for Image Steganography Technique", International journal of Next-Generation computing (ISSN: 2229-4678 (Print) and 0976-5034 (Online)), Vol. 8 no. 2, pp. 127-139, July 2017.
6. M. B. Medeni and E. M. Souidi, "A noval Steganographic method for gray level images with four pixel differencing and LSB substitution", (2010).
7. E. Cole, "Hiding in Plain Sight: Steganography and the Art of Covert Communication", Indianapolis: Wiley Publishing, (2003).
8. F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding- A Survey", Process of IEEE, vol. 87, no. 7, (1999) July, pp. 1062-1078.
9. K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran and B. S. Manjunath, "Steganalysis of quantization index modulation data hiding", Proc. of 2004 IEEE International Conference on Image Processing, vol. 2, (2004), pp. 1165-1168.
10. M. Warkentin, M. B. Schmidt and E. Bekkering, "Steganography and steganalysis", Premier reference Source–Intellectual Property Protection for Multimedia Information technology, Chapter XIX, (2008), pp. 374-380.
11. N. N. El-Emam, "Hiding a large amount of data with high security using steganography algorithm", Journal of Computer Science, vol. 3, (2007).
12. V. Kumar and S. K. Muttoo, "A Graph Theoretic Approach to Sustainable Steganography", MIS Review: An Int. Journal, vol. 17, no. 1, (2010), pp. 19-37.
13. Bhatia, M. P. S., Bhatia, M. K., and Muttoo, S. K. . "Secure Group message transferring stegosystem", International journal of information security and privacy, IGI global (ISSN: 1930-1650), Vol. 9 no. 4, pp. 59-76, 2015.
14. Bhatia, M. K, Muttoo, S. K. and Bhatia, M. P. S (2013). "Secure group communication with hidden group key", Information security journal: a global perspective, Taylor and Francis (ISSN:1939-3555 EISSN:1939-3547), Vol. 22 no.1, pp.21-34, 2013.
15. Bhatia, M. P. S, Muttoo, S. K. and Bhatia, M. K (2014). "An Image Steganography Method Using Spread Spectrum Technique" in Springer sponsored International Conference on Soft Computing for Problem Solving (SocProS 2014) organized by NIT SILCHAR, Assam, India in 2014, pp:219-236.