Secure Image Steganography using N-Queen Puzzle and its Comparison with LSB Technique

Akashdeep Singh
Department of Computer Science and Engineering
BBSBEC, Fatehgarh Sahib, Punjab, India

Sandeep Kaur Dhanda
Department of Computer Science and Engineering
BBSBEC, Fatehgarh Sahib, Punjab, India

Rupinder Kaur
Department of Computer Science and Engineering
BBSBEC, Fatehgarh Sahib, Punjab, India

Abstract- Steganography is the art of concealing the existence of information within seemingly harmless carriers. A message in cipher text may arouse suspicion while an invisible message will not. A digital image is a flexible medium used to carry a secret message because the slight modification of a cover image is hard to distinguish by human eyes. In this paper, we propose a method of image steganography using the N-Queen solution key. The experimental results are compared using MSE, PSNR and SNR parameters. The proposed scheme is secure because the intruder cannot directly tell the existence of data hidden inside the image.

Keywords – Steganography, LSB, MSE, PSNR, SNR.

I. INTRODUCTION

Steganography is the art and science of writing hidden messages [7] in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Stegnography is the process of hiding the one information into the other sources of information which can be a text, image or audio file[4] such that it is invisible in the natural view. Steganography supports different types of digital formats that are used for hiding the data. Depending upon the redundancy of the object the suitable format is used.

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 hide the hidden data, which may also be encrypted using the stego key. The resultant file is the stego medium same type of file as the cover medium. The cover mediums are typically image or audio files. LSB substitution is one of the classic image steganography approaches [6].

II. RELATED WORK

Image Steganography is the method of hiding the presence of data in cover images. Sanmitra Ijeri et.al, [9] propose the revised version of Roshan Shetty B R et.al. in which only one type of digital media was embedded in single cover image. But in proposed system multiple digital media can be embedded in single cover image. In proposed system, before embedding, the secret data is compressed and encrypted so that more and variable digital media are shared with more security. Since RED, GREEN & BLUE components of cover image pixel are used, the embedding capacity per pixel is 4.5 bits. The reference matrix used is of order 9 X 9. By using reference matrix, candidate elements (CEH, CEV, CEB) are chosen in such way that less distortion is produced in cover image after embedding the data. System provides two layer security one by using a random Sudoku among 6.671x1021 possible solutions and other by using strong encryption algorithm. The DES technique is used for encryption and the LSB technique is used for embedding the data into Sudoku puzzle. Sudoku solution is retrieved by decrypting Sudoku.

III. PROPOSED METHOD

The proposed method hides the secret message with minimum use of the LSB and using the N-Queen matrix as the solution key. The method is proposed to provide better security, an extra layer of data compression is added on the top .We are compressing our data using Arithmetic coding(AC) which results into a decimal number of range [0,1). For now, length of our input message can be up to 15 characters used to hide the secret messages by the following steps shown in figure:

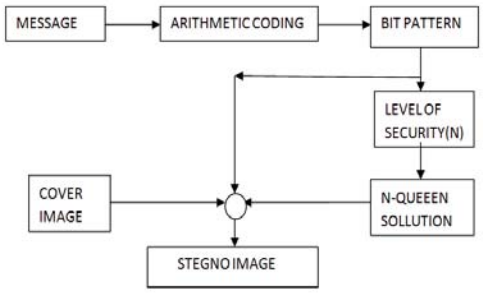

Figure 1.2 proposed method

Arithmetic Coding

In arithmetic coding, a message is represented by an interval of real numbers between 0 and 1. As the message becomes longer, the interval needed to represent it becomes smaller, and the number of bits needed to specify that interval grows. Successive symbols of the message reduce the size of the interval in accordance with the symbol probabilities generated by the model. The more likely symbols reduce the range by less than the unlikely symbols and hence add fewer bits to the message [5-6].

Before anything is transmitted, the range for the message is the entire interval [0, l] denoting the half-open interval 0.5 x < 1. As each symbol is processed, the range is narrowed to that portion of it allocated to the symbol.

Arithmetic code is converted to bit pattern

The arithmetic code is converted to bit pattern form.

Level of Security

For N-Queen puzzle the numbers of solutions are increasing with increase in 'n'. The level of security is directly proportional to N because the probability of selecting a solution is decreasing with increase in value of N.

If we choose level of security as 4, the image is divided into 16 chunks and each chunk will accommodate 4 bits. If we choose level of security as 8, the image is divided into 8 chunks and each chunk will accommodate 8 bits. If we choose level of security as 16, the image is divided into 4 chunks and each chunk will accommodate 16 bits.

Table no. 1 No. of N-Queen solutions

n	1 2 3 4 5	6 7	8	11	12	14	 25	26
Unique Solution	1 0 0 1 2	1 6	1 2	34 1	1,78 7	45,7 52	.... 275,986,683,74 .. 3434	2,789,712,466,5
Distinct Solution	1 0 0 2 1	4 4	9 2	2,6 80	14,2 00	365,5 96	... 2,207,893,435 .. 808,352	22,317,699,616, 364,044

Encoding Algorithm

Step 1. Set low to 0.0
Step 2.Set high to 1.0
Step 3.While there are still input symbols do
get an input symbol
Code range = high - low.
Step 4. High = low + range*high range(symbol)
Step 5. Low = low + range*low range(symbol)
End of While
Step 6. Output low.

Data Extraction

This is the final and the last step of the proposed method in which we have to decode the secret message from the image. Now we have stegano image and we want to retrieve the original message from the stegano image. We have the stegano image and the N-queen solution. From these two, we can find the bit pattern. After getting the bit pattern, we apply arithmetic decoding and we get the original message.
The following figure depicts the data extraction process.

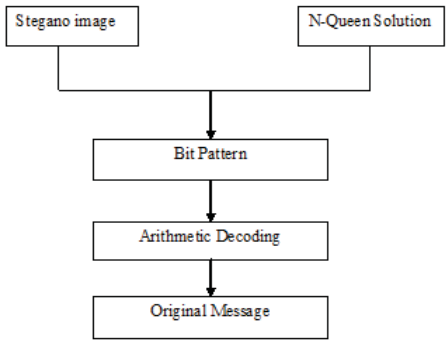

Figure 1.3 Data extraction

Decoding Algorithm

Step 1. get encoded number
Step 2. Do
find symbol whose range straddles
Step 3. the encoded number

output the symbol
range = symbol low value - symbol
Step 4. high value
subtract symbol low value from
Step 5. encoded number
divide encoded number by range
Step 6.until no more symbols.

IV. EXPERIMENTAL RESULTS

The distortion in cover image depends upon the change in value of pixels and number of pixels of cover image used for embedding which in turn depends upon the number of components of the pixel used and amount of input data. We use PSNR, SNR and MSE to evaluate the quality of an image. The PSNR is defined as follows

$$PSNR=10\cdot\log10\ \frac{255^2}{MSE}\ db.$$

PSNR is the Peak signal to noise ratio. As the value of PSNR increases the quality of the image improves and as the PSNR range decreases therefore the quality of the image decreases
Where MSE is the mean square error between the original image and the stego image. The MSE is defined as follows:

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

As the range of MSE increases the quality of the image decreases and as the range of MSE decreases the quality of the image improves.
And SNR is Signal to Noise ratio of the image and is defined as follows

$$SNR=10\cdot\log10\ \frac{P\ signal}{P\ noise}$$

As the value of SNR increases the quality of the image decreases and as the value of SNR decreases the quality of the image improves.

Table 3: Image comparison with LSB

Image	PSNR Using N-Queen	MSE Using N-Queen	PSNR Using LSB	MSE Using LSB
Flower Image	53.6927	0.2778	46.4978	1.4565
Car Image	57.5628	0.0773	46.2428	1.5445

Figure 1.4 Image before embedding

Figure 1.5 Image after embedding

V. CONCLUSION

Steganography is the science of secret data delivery. The paper is to develop a method of steganography in which key is used to select embed position .System provides two layer security one by using a random N-Queen solutions and other by making minimum use of the LSB technique. The proposed system can be used in the fields where more priority is given to security instead of amount of data shared. So this can be used in wide range of applications like military, medical imaging, banking etc, since the quality of the image is not affected much, before and after embedding. From the table it is clear that with the decrease in MSE value the PSNR value is increased and therefore the quality of the image is also improved to that of the original image.

VI. FUTURE SCOPE

There could be lot of scope for further enhancement to this project, some of which are listed here.

1. In this proposed method we have modified only the 64 bits of the image. More bits of the image can also be modified. In that way a higher embedding capacity can be obtained.
2. Two or more digital media files (input files) can be embedded in a single image file.

REFERENCES

[1] Chin-Chen Chang, Yung-Chen Chou and The Duc Kieu, High Capacity Data Hiding for Grayscale Images , The First International Conference on Ubiquitous Information Management and Communication, Seoul, Korea, 2007, pp 139-148.

[2] Mamta Juneja, Parvinder Singh Sandhu, Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp 302-305.

[3] Roshan Shetty B R, Rohith J, Mukund V, Rohan Honwade, Shanta Rangaswamy, Steganography using Sudoku Puzzle, International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp 623-626.

[4] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, Application of LSB Based Steganographic Technique for 8-Bit color image, World Academy of Science, Engineering and Technology, 2009, pp 423-425.

[5] Piyush Marwaha, Paresh Marwaha, visual cryptographic steganography technique, second International conference on Computing, Communication and Networking Technologies, 2010, pp 1-6.

[6] Tao Zhang, Wenxiang Li, Yan Zhang, Xijian Ping, Detection of LSB Matching Steganography Based on Distribution of Pixel Differences in Natural Images, Zhengzhou Information Science and Technology Institute Zhengzhou, China,2010, pp 1-5.

[7] Ge Huayong, Huang Mingsheng, Wang Qian, Steganography and Steganalysis Based on Digital Image, 4th International Congress on Image and Signal Processing, 2011, pp 252-255.

[8] S. Changder, N. C. Debnath, D. Ghosh, , A greedy approach to text steganography using properties of sentences, Eighth International Conference on Information Technology: New Generations, 2011, pp 30-35.

[9] Sanmitra Ijeri, Shivananda Pujeri, Shrikant B, Usha B A, Image Steganography using Sudoku Puzzle for Secured Data Transmission, International Journal of Computer Applications , 2012, pp 32-35.

[10] Rupinder Kaur, Deepak Aggarwal, Analysis of Secure Text Embedding using Steganography, International Journal of Latest Trends in Engineering and Technology,2013,pp 120-126.