A N-QUEEN BASED POLYNOMIAL APPROACH FOR IMAGE STEGANOGRAPHY

G.Manikandan [#1], S.Ramakrishnan [#2], Baburam Sathiya Nijanthan.P [#3], Harikrishnhaa.R [#4]

[#] School of Computing, SASTRA University,
Thanjavur, India – 613401
[1] manikandan@it.sastra.edu
[2] srk@ict.sastra.edu
[3] baburam1803@gmail.com
[4] harikrishnhaa@gmail.com

Abstract: **The objective is to generate a polynomial based on the cover image with the help of an 8-Queens Algorithm and Discrete Cosine Transform (DCT). By segmenting the image into 64 parts and applying DCT for every segments, a set of 64 DC coefficient values are obtained. Using mapper, these DC values are scrambled. The initial position of the Queen is given to 8-Queens Algorithm which generates the solution. Using the calculated DCT values and the position of the Queen obtained, the polynomial equation is generated which can be used for embedding and extraction of information.**

Keywords: N-Queen, Polynomial, Image Steganography

I. INTRODUCTION

Steganography is an art in which data can be shared in a secret way between intended persons in such a way that data is embedded inside a multimedia like image, audio and video. Unlike cryptography and watermarking, steganography has an added advantage that the intruder cannot detect the data at the first sight since the data present in the media is invisible. Steganography has various number of security applications that can be used between individuals, groups and agencies. Steganography can be categorized into two types. They are Linguistic Steganography and Technical Steganography. In Technical Steganography, data is embedded into Digital media like images, audio, video, text. Linguistic steganography is a non-technical way of representing an information in a cover. For example, the sender writes the secret message into the holes by placing his mask over a sheet of paper and then compose a cover message by filling the remaining part of the paper with some random texts. The receiver can read the same message by placing the same mask over the received cover [7].

II. LITRATURE REVIEW

In the year 2011, Soniya Vijayakumar has proposed a steganographic approach using linear and quadratic polynomials for random selection of bytes from an image to store the text in a better and stronger manner [1].

Security is enhanced by integrating the key features of compression, cryptography and steganography [2].

In the year 2012, Karthikeyan et al., has proposed a Pseudo randomized key generation approach to improve the efficiency of steganographic approach and also strengthening the security by processing the image pixels with some scanning methods [3].

G.Manikandan et al., has proposed a hybrid approach which involves both an effective steganographic and cryptographic methods based on the Discrete Wavelet Transform to increase the efficiency and reduce the size of the stego image [4].

Po-Yueh Chen et al., has proposed a steganography system to embed data in Frequency domain efficiently using Discrete Wavelet Transforms due to difference characteristics of DWT coefficients in different sub bands and respectable security is maintained [5].

In the year 2010, Abbas Cheddad et al., has done survey about several steganographic methods and discussed about major algorithms in steganography which can be deployed in a digital image. [6].

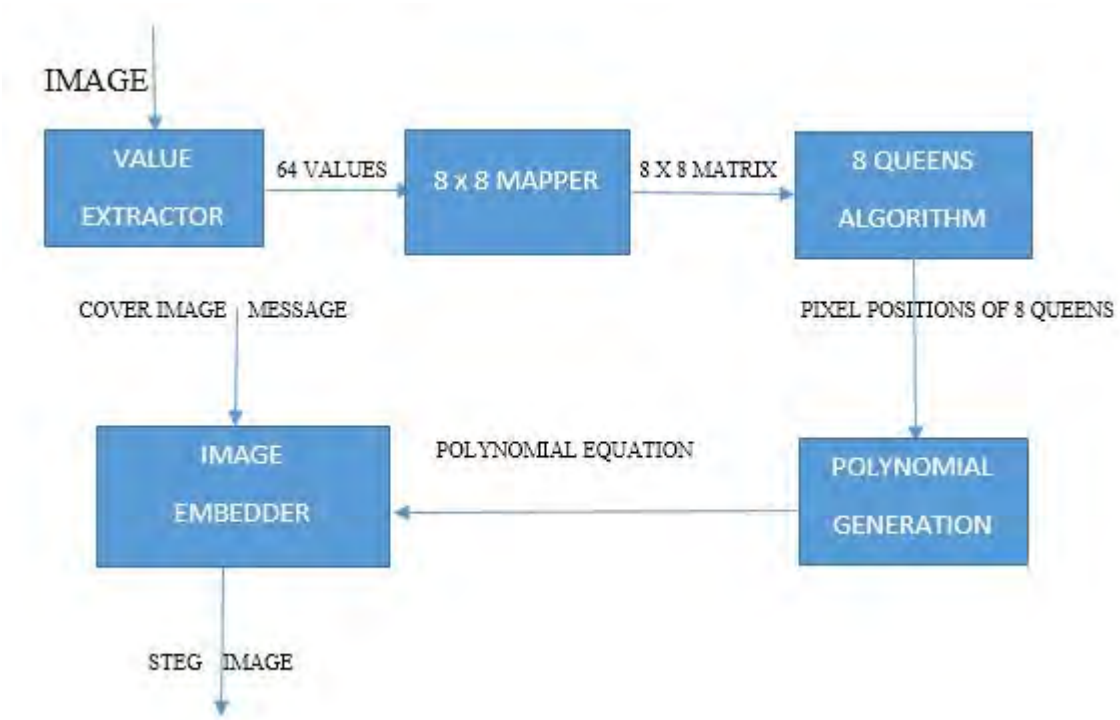
Amirtharajan et al, proposed a steganographic technique to embed the message on blue and green plane based on the intensity value of red plane to increase the secrecy, robustness, randomness and imperceptibility. [8].

III.PROPOSED SYSTEM

In a polynomial based steganography, there exists a difficulty in generating the polynomial and how to share it efficiently between the sender and the receiver. When a polynomial with small degree is taken, embedding and extraction can be done easily but the chances of intruder's attack will be more whereas when a polynomial with high degree is taken, the chances of intruders attack is less compared to the previous one but the computations will be more.

In our approach, Polynomial which is used for embedding and extraction is generated using the cover image by using 8-Queen's Algorithm and Discrete Cosine Transform. In the first stage, the image is segmented into 64 equal parts. After segmentation is done, Discrete Cosine Transform is applied to each part and DC coefficient (First value of the DCT matrix) is obtained. By giving mapper position and mapper value the 64 DC coefficients are shuffled and mapped into 8 X 8 Mapper. Once all 64 values are mapped inside the mapper, 8 Queens Algorithm is applied. An 8 Queens Algorithm is nothing but 8 Queens are placed in chess board in such a manner that no Queen should conflict with each other. Here in this system, the initial position of the Queen is given and using this initial position the first solution for that position is obtained. By using these positions of 8 Queens and their respective DC coefficient values, polynomial is generated which is used for the embedding and the extraction of the message.

A. Block Diagram:



1) *Value Extractor:*

The taken cover image is segmented into 64 segments and DCT of each segment is calculated by leaving the last bit of the pixel (As we will embed data in this bit). 64 values are generated from the DC coefficients of each segment's DCT values.

2) *Mapper:*

The generated 64 values are scrambled using the mapper value and mapper position given by the user let it be 'm_val' and 'm_pos'. An array with 1 to 64 values is taken and the mapper position and mapper value is swapped in that array. We will start from mapper position and skip the next 'm_val' number of values and successive value is taken as first value in scrambled matrix .This process is done until all 64 values are scrambled. Then the 64 values are reshaped into a block of 8 X 8 mapper matrix.

3) *8 Queen's Algorithm:*

. In 8 Queen's algorithm we have to place 8 queens in an 8 X 8 board such that the queen is placed in each row not conflicting with any other queen. For particular Queen Position the solution for 8 Queen's Algorithm is generated by backtracking mechanism. Queen is placed in n^{th} row by not conflicting with any other queens that have been already placed in (n-1) rows. If there is no other possibility for placing the queen in row n, then we will change the position of queen in the $(n-1)^{th}$ row and try to find the solution.

4) *Polynomial Generator:*

64 values generated from mapper and solution from 8 queen's algorithm is compared to generate the polynomial. Whenever a queen is present in a row the corresponding value in mapper matrix is taken for generating the polynomial. The row positions is taken as degree of that polynomial and corresponding DC coefficients are taken as the coefficient for their respective degree of the polynomial

5) *Image Embedder:*

In this block the message is added to the cover image with the help of the polynomial equation using 1-bit LSB substitution method as follows:

The value of the polynomial is found by giving the message bit position as input and modulo TEN operation is performed to get a value **'n'**. Then we will embed the data in the n+1th byte of the cover image using following formula.

S=C - C MOD 2 + M

Where,

S is the Stego Image, **C** is the Cover Image, and **M** is the message to be embedded in decimal,

6) *Extraction Phase:*

In receiver side all the blocks discussed above are carried down and the message is extracted from Stego Image as follows:

M = S MOD 2

Where,

S is the Stego Image, and **M** is the secret message,

B. Procedure:

Step1: Choose the cover image

Step2: Give the initial position of the Queen, mapper position, mapper value as inputs.

Step3: Input the message to be embedded in the cover image.

Step4: Generate the polynomial by using three input parameters and by using that polynomial, embed the message in the image.

Step5: Send the stego image to the receiver.

Step6: Receive the stego image and give those three input parameters and message length in the receiver's side to generate the same polynomial

Step7: Extract the message using that polynomial

Step8: Display the message in the receiver's side.

IV.CASE STUDY AND SIMULATION

The above approach has been implemented using the platforms java developer kit 1.4 and mat lab R2009a. The minimum system requirement to execute the results and simulation is to have minimum of 1GB Ram and Core 2 duo Processor.

Fig. 1 depicts the cover image which is used in this approach. Three input parameters and message which is to be embedded is given by the user as depicted in Fig. 2.

Fig. 1

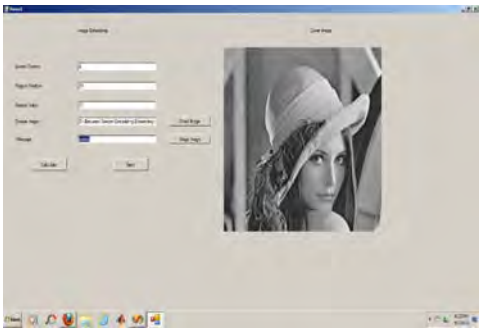


Fig. 2

Using the mapper position and mapper value, the DC coefficients are scrambled and reshaped as an 8 x 8 matrix as shown in fig. 3 and with the help of initial queen position, the 8-queen solution matrix is generated as depicted in fig. 4. By comparing this solution with the scrambled DC coefficient matrix with solution matrix, the corresponding DC coefficient values in DC coefficient matrix are taken where the queen is present in the solution matrix and it is used as a coefficient to the polynomial and the respective row position as the degree to the polynomial which will generate the coefficient of the polynomial with increasing degree as shown in Fig. 5.

678	568	503	578	1097	544	456	716
350	7	447	474	482	453	455	826
637	986	225	917	666	72	556	351
726	437	596	445	13	787	513	525
241	835	436	127	246	249	567	499
533	352	370	469	565	373	311	957
476	503	538	529	586	593	480	152
587	627	101	354	581	338	508	61

Fig. 3

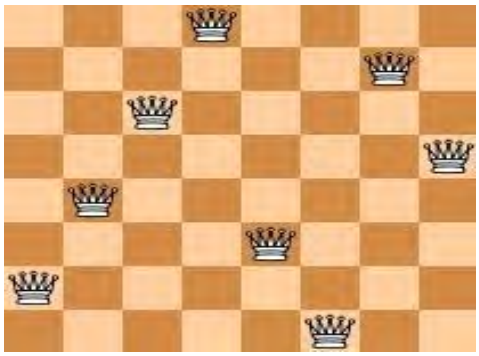


Fig. 4

578 826 637 596 249 352 480 581

Fig. 5

Using that polynomial, the message is embedded in the image and the resultant image is a stego image which is depicted in fig. 6. On the receiver's side, as shown in fig. 7, the above input parameters that is initial position of the queen, mapper position and mapper value is given and length of the message is also given to generate the same polynomial for the extraction purpose.

Fig.6

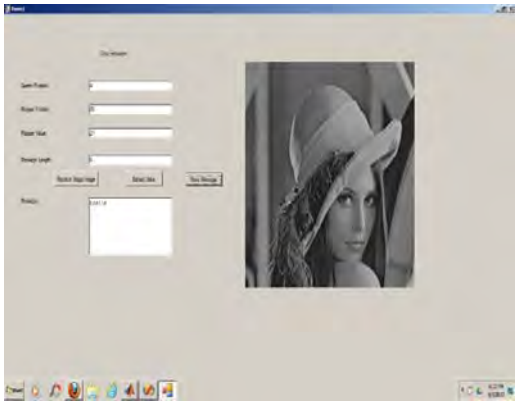


Fig. 7

Through experiments it is found that by taking 1 MB data and embedding it in 512 x 512 Lena image (cover) the obtained Mean Square Error is 0.0127 and Peak Signal to Noise Ratio is 67.0944.

V. CONCLUSION

In this paper, we have proposed a new technique for image steganography that improves the security over the existing system. Here, instead of using the conventional methodology of directly sharing the polynomial, the polynomial is generated using the cover image with the help of 8 Queens Algorithm and Discrete cosine transform. Apparently, we share only the initial position, mapping position and mapping value which makes it difficult for the intruder to find out the method of the polynomial generation using these three parameters. Thus, the above method increases the security without compromising the accuracy.

REFERENCES

[1] Ms. Soniya Vijayakumar, "Image Steganography based on Polynomial Functions", Journal of Global Research in Computer Science, vol. 2(3), March 2011.

[2] G.Manikandan, N.Sairam, M.Kamarasan, "A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme", Research Journal of Applied Sciences, Engineering and Technology, vol. 4(6) 2012.

[3] B.Karthikeyan, V.Vaithiyanathan, B. Thamotharan, M.Gomathymeenakshi and S.Sruthi, "LSB Replacement Stegnography in an image Using Psudorandomised Key Generation". Research Journal of Applied Sciences, Engineering and Technology, vol. 4(5), pp. 491-494, 2012.

[4] G.Manikandan, M.Kamarasan and S.Sairam, "A New Approach for Secure Data Transfer based on Wavelet Transform". International Journal of Network Security, vol. 15(2), pp. 106-112, 2013.

[5] P. Chen and H. Lin, "A DWT Based Approach for Image Steganography," International Journal of Applied Science and Engineering, vol. 4(3), pp. 275-290, 2006.

[6] Abbas Cheddad, JoanCondell, KevinCurran, PaulMcKevitt "Digital image steganography: Survey and analysis of current methods", vol. 90, pp. 727–752, 2010.

[7] Stefan Katzenbeisser and Fabien A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking"

[8] Rengarajan Amirtharajan, Aishwarya G, Madhumita Rameshbabu, John Bosco Balaguru Rayappan, "Optimum Pixel & Bit location for Color Image Stego- A Distortion Resistant Approach", International Journal of Computer Applications, vol. 10(7), 2010.