Dr.Ch.BalaSwamy, Pasumarthy Sarada / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.2741-2744

Improving Image Data Hiding Capacity Scheme using Sudoku Puzzle in Color Images

Pasumarthy Sarada[#1], Dr.Ch.BalaSwamy [*2]
M.Tech (DECS) Student, Dept. Of ECE, QIS College of Engineering & Technology
Pondur Road, Ongole-523272, India.
* Professor, HOD of ECE, QIS College of Engineering & Technology
Pondur Road, Ongole-523272, India.

Abstract:-Steganography is a skill to convey the secret data in the digital images without getting any unexpected notices to attackers. LSB replacement, the simplest method, directly replaces the secret bits with LSB bit plane. Unfortunately, it is insecure because it cannot resist against the visual attacks and statistic detection. The original work was proposed by Chang et al. in 2010, and their work was inspired by Zhang and Wang's method and Sudoku solutions. Chang et al. successfully used Sudoku solutions to guide cover pixels to modify pixel values so that secret messages can be embedded. The main idea of our scheme is to use a Sudoku puzzle, in which every value corresponds to a pixel pair (red, blue) of image mapped with the secret digit by replacing a pair of one pixel of two colors. Experimental results show that the proposed scheme can improve the visual quality of stego-images. In addition, the average of hiding capacity is 4 bpp (bits per pixel). Therefore, it confirms that our proposed scheme provides higher hiding capacity than that of existed Scheme (Chang et al). Furthermore, our method shows the positive results to resist against the visual attacks. Moreover, the proposed scheme provides a large capacity for embedded secret data. The earlier version is for a grayscale image but the proposed method is for a colored image.

Keywords- Data hiding, Steganography, Sudoku, Reference Matrix, Secret data, Sudoku

I Introduction:

By the use of Computer and the expansion in different areas of life and work, the issue of security of information has gained special significance. One of the concerns in the area of information security is the concept of hidden exchange of information. For this purpose, various methods including cryptography, steganography, coding and so on have been used. Steganography is one of the methods which have attracted more attention during the recent years.

In Steganography the information is hidden in cover media so nobody notice the existence of the secret information. Steganography works have been carried out on digital media such as images, sounds and videos.

Sudoku has become a worldwide puzzle craze within the past year. Previously known primarily in Japan, it now graces newspapers, Web sites, and best-selling books in dozens of countries. A puzzle consists of a 9-by-9 grid made up of nine 3-by-3 subgrids. Digits appear in some squares, and based on these starting clues, a player completes the grid so that each row, column, and subgrid contains the digits 1 to 9 exactly once. An easy puzzle requires only simple logical techniques-is a subgrid needs an 8, say and two of the columns running through it already hold an8, then and subgrid's 8 must go in the remaining column. A hard puzzle requires more complex pattern recognition skills; for instance, if a player computes all possible digits for each cell in a subgrid and notices that two cells have exactly the same two choices, those two digits can be eliminated from all other cells in the subgrid.

A computer solves a 9-by-9 sudoku within a second by using logical tricks that are similar to the ones humans use, but finishes much faster. On a large scale, however, such shortcuts are not powerful enough and checking the explosive number of combinations becomes impossible, even for the world's fastest computers. And no one knows of an algorithm that's guaranteed to find a solution without trying out a huge number of combinations. This places Sudoku in an infamously difficult class, called NP-complete, that includes problems of great practical importance, such as scheduling, network routing and gene sequencing.

Two important factors needed to consider when we are designing a new information hiding scheme are embedding capacity (i.e. the number of secret bits can be embedded into one cover pixel) and visual quality of stego images (i.e. image distortion). Desirably, one would want to achieve high embedding capacity and good visual quality. However, embedding capacity and visual quality are inversely proportional to each other. That is, if embedding capacity is increased, then visual quality is decreased and vice versa. Thus, a tradeoff between embedding capacity and visual quality is made by users for different applications[1].

The main objective of this paper is to improve the efficiency of the previously proposed method so as to make it possible to be implemented in the normal desktop computer without considering main memory and also to extend the digital media cover image from grey scale to RGB image (color image).

II Related Work:

In this section, we will briefly describe Shanta Rangaswamy's work on steganographic schema based on Sudoku solutions. The central idea of Rangaswamy is to modify the pixels if an image using a 9×9 sudoku based on specially designed reference matrix M[1]. To design a reference matrix, a "tile" matrix T is constructed first by subtracting every digit in a sudoku puzzle by one, os that the digits in matrix T ranged from 0 to 8. The reference matrix M is then consisteing of an m×m tiling of copies of T, where m= └256/16┘

III. Proposed Work

Steganography using hexa Sudoku is used to hide digital data or information into an image using Sudoku solution. This method is using 24 bit of any type of image. This method is modifying 16 bits of each pixel of image. The secret data is converted to Base-16 for mapping them into Hexadecimal Sudoku solution as shown in Fig 1. In the Sudoku solution every value is subtracted by 1 called Tile Matrix. To ensure that all values between 0 to 15 in Sudoku as shown in Fig 2, for maintaining compatibility between secret data and the Sudoku values. This Sudoku solution is then expanded to 256 X 256 matrix called reference matrix (M) as shown in Fig. 3.

5	8	4	10	6	A	B	7	3	B	C	F	1	8	D	0
E	2	F	9	4	C	B	3	10	1	5	D	5	9	7	6
C	7	6	1	8	F	5	9	4	2	E	A	2	C	A	F
A	B	D	3	E	1	2	10	6	9	8	7	4	E	3	B
F	1	3	A	10	2	7	E	D	4	6	C	8	5	9	B
4	D	10	2	C	5	1	A	9	8	F	B	E	7	6	3
9	5	7	B	3	8	F	6	2	E	10	1	C	4	D	A
6	E	C	8	9	D	4	B	5	7	A	3	F	1	10	2
3	A	8	7	5	E	9	1	F	C	D	6	B	10	2	4
B	4	E	C	7	6	3	F	1	10	9	2	A	8	5	D
2	F	9	6	A	10	C	D	B	5	4	8	1	3	7	E
D	10	1	5	2	B	8	4	A	3	7	E	9	6	C	F
7	6	A	D	1	9	E	C	8	F	B	10	4	2	3	5
8	9	5	F	B	3	10	2	C	D	1	4	7	E	A	6
1	3	B	4	D	7	A	8	E	6	2	5	10	C	F	9
10	C	2	E	F	4	6	5	7	A	3	9	D	B	1	8

Fig 1: 16×16 Sudoku

4	7	3	F	5	9	C	6	2	A	B	E	1	8	D	0
D	1	E	8	3	B	A	2	F	0	4	C	5	9	7	6
B	6	5	0	7	E	4	8	3	1	D	9	2	C	A	F
9	A	C	2	D	0	1	F	5	8	7	6	4	E	3	B
E	0	2	9	F	1	6	D	C	3	5	B	7	4	8	A
3	C	F	1	B	4	0	9	8	7	E	A	D	6	5	2
8	4	6	A	2	7	E	5	1	D	F	0	B	3	C	9
5	D	B	7	8	C	3	A	4	6	9	2	E	0	F	1
2	9	7	6	4	D	8	0	E	B	C	5	A	F	1	3
A	3	D	B	6	5	2	E	0	F	8	1	9	7	4	C
1	E	8	5	9	F	B	C	A	4	3	7	0	2	6	D
C	F	0	4	1	A	7	3	9	2	6	D	8	5	B	E
6	5	9	C	0	8	D	B	7	E	A	F	3	1	2	4
7	8	4	E	A	2	F	1	B	C	0	3	6	D	9	5
0	2	A	3	C	6	9	7	D	5	1	4	F	B	E	8
F	B	1	D	E	3	5	4	6	9	2	8	C	A	0	7

Fig 2: Tile Matrix.

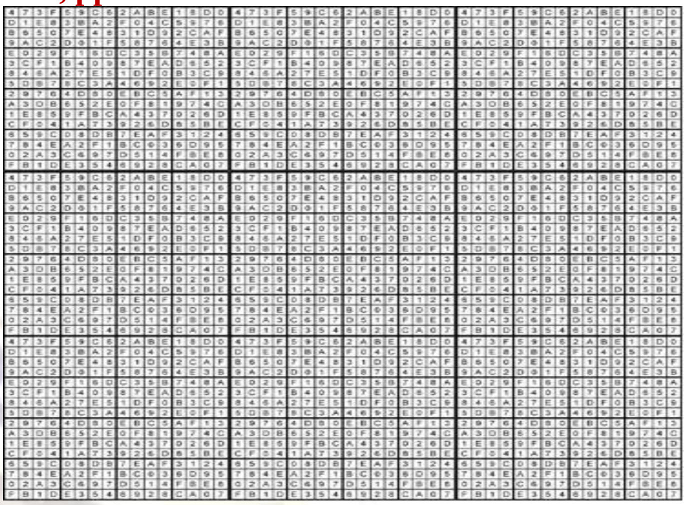

Fig. 3. 255 X 255 Refe**rence Matrix(M)**

1.Data Embedding:

In the data embedding phase, first convert the secret bit stream into secret digits in the base-16 numeral system, and then embed these secret digits into the cover image. Suppose the converted secret digits are denoted by $S=s_1s_2s_3\ldots.s_n$, where n is the total number of converted secret digits and $s_k \in [0, 15]$, $1\leq k\leq n$. During embedding, consider two color values from pixel (Red & Green). As it is known that each of the pixel color value has a value ranging from 0 to 255, these pixel color values are selected and they are used as x and y co-ordinate values to locate the position in the reference matrix.

We find the value in the reference matrix at that position pointed by the pixel color values and the secret digits that have to be embedded are selected and the closest position of the secret digit to that of the pointed values is selected and the pixel values are modified to the new values.

2.Data Extraction:

The embedded data can be extracted directly from the stego image by referencing the same Sudoku solution used in the embedding phase. The pixel color pair is chosen and the secret digit is simply obtained by referencing the reference matrix M at the position using the pixel values as the co-ordinate values.

IV. Mathematical Representation

(i)*Data Embedding*

An image on which the secret data to be embedded is selected. Each pixel of the image is extracted, and the red, green color of the image pixels. The range of value are from 0 to 255.

Now the values of R,G are represented as g_i ,g_{i+1}, then three candidate elements are chosen called horizontal(CE_H), vertical(CE_V), boxed(CE_B). The required formulae for selecting values from the reference matrix are as follows:

Necessary Formulae:

S1:(i.e. select the candidate elements for CE_H)

If $g_{i+1} > 5$and $g_{i+1} < 246$ then

$CE_H = \{M(g_i, gi+1 - 5), M(gi, g_{i+1}- 4), M(g_i, g_{i+1}- 3), M(g_i, g_{i+1} - 2), M(g_i,g_{i+1}-1), M(g_i, g_{i+1}), M(g_i, g_{i+1} + 1), M(g_i, g_{i+1} +2), M(g_i, g_{i+1} +3), M(g_i, g_{i+1} +4), M(g_i, g_{i+1} +5), M(g_i, g_{i+1} +6), M(g_i, g_{i+1} +7), M(g_i, g_{i+1} +8), M(g_i, g_{i+1} +9), M(g_i, g_{i+1} +10)\}$;

Else If $g_{i+1} \leq 5$ then

$CE_H = \{M(g_i, g_{i+1}), M(g_i, g_{i+1}+1), M(g_i, g_{i+1}+2), M(g_i, g_{i+1}+3), M(g_i, g_{i+1}+4), M(g_i, g_{i+1}+5), M(g_i, g_{i+1}+6), M(g_i, g_{i+1}+7), M(g_i, g_{i+1}+8), M(g_i, g_{i+1}+9), M(g_i, g_{i+1}+10), M(g_i, g_{i+1}+11), M(g_i, g_{i+1}+12), M(g_i, g_{i+1}+13), M(g_i, g_{i+1}+14), M(g_i, g_{i+1}+15)\}$

Else If $g_{i+1} \geq 246$ then

$CE_H = \{M(g_i, g_{i+1}), M(g_i, g_{i+1}-1), M(g_i, g_{i+1}-2), M(g_i, g_{i+1}-3), M(g_i, g_{i+1}-4), M(g_i, g_{i+1}-5), M(g_i, g_{i+1}-6), M(g_i, g_{i+1}-7), M(g_i, g_{i+1}-8), M(g_i, g_{i+1}-9), M(g_i, g_{i+1}-10), M(g_i, g_{i+1}-11), M(g_i, g_{i+1}-12), M(g_i, g_{i+1}-13), M(g_i, g_{i+1}-14), M(g_i, g_{i+1}-15)\}$

S2: (i.e. select the candidate elements for CE_V)

If $g_i > 5$and $g_i < 246$, then

$CE_V = \{M(g_i -5, g_{i+1}), M(gi-4, g_{i+1}), M(g_i-3, g_{i+1}), M(g_i-2, g_{i+1}), M(g_i -1,g_{i+1}), M(g_i, g_{i+1}), M(g_i+1, g_{i+1}), M(g_i +2, g_{i+1}), M(g_i +3, g_{i+1}), M(g_i +4, g_{i+1}), M(g_i +5, g_{i+1}), M(g_i +6, g_{i+1}), M(g_i +7, g_{i+1}), M(g_i +8, g_{i+1}), M(g_i +9, g_{i+1}), M(g_i +10, g_{i+1})\}$

Else If $g_i \leq 5$, then

$CE_V = \{M(g_i,g_{i+1}), M(g_i+1,g_{i+1}), M(g_i+2,g_{i+1}), M(g_i+3,g_{i+1}), M(g_i+4,g_{i+1}), M(g_i+5,g_{i+1}), M(g_i+6,g_{i+1}), M(g_i+7,g_{i+1}), M(g_i+8,g_{i+1}), M(g_i+9,g_{i+1}), M(g_i+10,g_{i+1}), M(g_i+11,g_{i+1}), M(g_i+12,g_{i+1}), M(g_i+13,g_{i+1}), M(g_i+14,g_{i+1}), M(g_i+15,g_{i+1}) \}$;

Else If $g_i \geq 246$

$CE_H = \{M(g_i-1, g_{i+1}), M(g_i-2, g_{i+1}), M(g_i-3, g_{i+1}), M(g_i-4, g_{i+1}), M(g_i-5, g_{i+1}), M(g_i-6, g_{i+1}), M(g_i-7, g_{i+1}), M(g_i-8, g_{i+1}), M(g_i-9, g_{i+1}), M(g_i-10, g_{i+1}), M(g_i-11, g_{i+1}), M(g_i-12, g_{i+1}), M(g_i-13, g_{i+1}), M(g_i-14, g_{i+1}), M(g_i-15, g_{i+1}), M(g_i-16, g_{i+1}) \}$.

S3: (i.e. select the candidate elements for CE_B)

If $g_i<251$ and $g_{i+1} <251$ Then

$x_b= \lfloor g_i/4 \times 4 \rfloor$, $y_b= \lfloor g_{i+1} / 4 \rfloor \times 4$

$CE_B =\{M(x_b,y_b),M(x_b,y_{b+1}), M(x_b,y_{b+2}), M(x_b,y_{b+3}), M(x_{b+1},y_b), M(x_{b+1},y_{b+1}), M(x_{b+1},y_{b+2}), M(x_{b+1},y_{b+3}), M(x_{b+2},y_b), M(x_{b+2},y_{b+1}), M(x_{b+2},y_{b+2}), M(x_{b+2},y_{b+3})\}$

Else CE_B is empty

Then location of each digit of secret information (which is in base-16) to be embedded is found with respect to R and G. According to an input secret digit S_i, three candidate elements $M(x_H, y_H)$, $M(x_V , y_V)$, and $M(x_B, y_B)$ are found from CE_H, CE_V , and CE_B, respectively. In other words, if g_i, and g_{i+1} are smaller than 255, then the found candidate elements satisfy $M(x_H, y_H) = M(x_V , y_V) = M(x_B, y_B) = S_i$; otherwise, $M(x_H, y_H) = M(x_V , y_V) = S_i$. The cover pixel pair (g_i, g_{i+1}) is modified as (g_{i1}, g_{i+11}) by a minimum distortion candidate element $M(x_{min}, y_{min})$ which is selected by using Manhattan distance formula:

$M(x_{min}, y_{min}) = min_j =H,V,B\{| g_i - x_j | + |g_{i+1} -y_j|\}$

Thus, the cover pixel pair (g_i, g_{i+1}) is modified as $(g`_i = x_{min}, g`_{i+1} = y_{min})$ to conceal the secret digit S_i with small distortion. This small distortion does not affect the image much and no physical difference can be identified of this image with respect to original image. After performing the above replacement for all digits of secret information the embedding phase is complete.

In this paper we will encrypt the given input string and then embedded the encrypted string rather than the original string which enhances the security of the data. The main requirement for this paper is that the Sudoku solution has to be same at both sender and receiver end. The size of secret information is embedded initially on the cover image so that receiver can determine how many pixels to scan and retrieve data. Since digital media can be any type of data such as text, image, audio etc; it is necessary for the receiver to be aware of it. This is done by embedding them after embedding secret digits on the cover image itself. This is done by embedding the size of extension followed by the extension itself.

(ii)Data Extraction:

The embedded secret digits can be exactly extracted from the received stego-image with the same Sudoku solution used in the embedding phase. In this phase first each pixel is extracted from the stego-image. Then from this red(R) and green (G) components of each pixel are used (similar to embedding phase).

The Sudoku solution which is shared between the user and the receiver is converted into a reference matrix (16×16 matrixes) by subtracting 1 from the Sudoku solution, similar to the one shown in fig b. The R and G are chosen as X-axis and Y-axis components of Sudoku solution, forming pair (g_i, g_{i+1}),where g_i = R and g_{i+1} = G. The value at position (g_i, g_{i+1}) is the required secret digit. This process is done for all pixels and data is extracted. The obtained secret digit (which is in base-16) is converted to base-9. This completes extraction phase.

V.Resulsts

Several Experimental Results were conducted to show the effectiveness of the proposed scheme.

In addition, the performance of safety is discussed. The quality of stego-image is evaluated using histogram comparison in MAT Lab and embedding capacity in terms of characters.

Proposed method explanation on image Lena:

Lena Image size=256 KB.

No. of Pixels in image=262144.

Proposed method embedding capacity=4 bpp.

For hiding one character=2 pixels required.

Therefore 262144/2=131072 character.

This method can hide 128 KB secret message in the above image (Lena).

Before embedding:

After embedding:

Histograms for the Lena (above) image:

Histogram:1 for the original, Histogram:2 for the image containing hidden text.

Histogram:1

Histogram:2

VI. Conclusion

Steganography, in its multitude of forms, has been in use literally for thousands of years. It appears to have been utilized primarily and most effectively in time of war or civil strife. It would appear that based on the variety of forms that steganographic messages can take that there could be steganographic content on the internet. This paper is improving the embedding capacity and distortion is very low compared with other existing methods and quality of image is also good. The hiding capacity of our proposed scheme is 4 bpp on average. Moreover, the results show the positive data to confirm its security. In the future, we extend this version to achieve higher hiding capacity as well as better visual quality.

References:

[1] C.-C. Chang, T. D. Kieu, and Y.-C. Chou. High capacity data hiding for grayscale images. In Proceedings of the First International Conference on Ubiquitous Information Management and Communication, pages 139–148. Seoul, Korea, February 2007.

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

[3] Y.-T. Wu and F. Y. Shih. Digital watermarking based on chaotic map and reference register. Pattern Recognition, 40(12):3754–3763, December 2007.

[4] C.C. Chang, Y.C. Chou and T.D. Kieu, An Information Hiding Scheme Using Sudoku, Proceedings of the Third International Conference on Innovative Computing, Information and Control (ICICIC2008), June 2008.

[5] B. Felgenhauer and F. Jarvis. Mathematics of Sudoku I, Mathematical Spectrum, vol. 39, no. 1, pp. 15-22, 2006. 626