Image Steganography using Sudoku Puzzle for Secured Data Transmission

Sanmitra Ijeri,
Final year B.E (CSE)
R.V College of Engineering
Bangalore, India.

Shivananda Pujeri,
Final year B.E (CSE)
R.V College of Engineering
Bangalore, India.

Shrikant B,
Final year B.E (CSE)
R.V College of Engineering
Bangalore, India.

Usha B A,
Asst.Prof.Departement of CSE R.V College Of Engineering
Bangalore, India.

ABSTRACT

Image Steganography is the method of hiding the presence of data in cover images .Here we propose the revised version of Roshan Shetty B R et al. whose work was inspired by C. Chang et al. In earlier work only the RED & GREEN components of cover image pixel was used and reference matrix used was of order 27 x 27 and embedding capacity was 3 bits per pixel. In this paper we use RED, GREEN & BLUE components of cover image pixel and reference matrix of order 9 x 9. Hence, the embedding capacity is 4.5 bits per pixel. Prior to embedding the data we use compression and encryption so that more and various digital media are securely embedded in cover image.

General Terms

Steganography, Embedding, Extracting, Compression, Encryption.

Key Terms

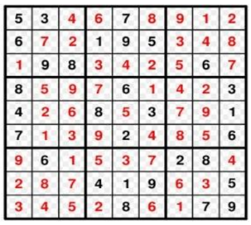
Secret data, Reference matrix, RGB, pixel, Cover image, Stego image.

1. INTRODUCTION

Using digital images as cover media to conceal secret data is an important issue for secret data delivery applications. From the target of image modification, information hiding techniques can be classified into three domains, namely spatial domain [1], compressed domain [2], and transformed domain [3]. In spatial domain, more redundant spaces are available to secret data embedding so high embedding capacity can be achieved, and less time is needed for embedding and extracting procedures. However, information hiding schemes in spatial domain are vulnerable to common attacks such as statistical stego analysis. So security in steganography can be achieved using different embedding schemes [4-5]. The 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 image pixel), visual quality of stego images [6] (i.e. image distortion); amount of data sent (i.e. compression) and secure exchange of data (i.e. Encryption). Desirably, one would want to achieve high embedding capacity, good visual quality, and more data to get embedded and high security. 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. The security and embedding more data can be done using encryption and compression. Section 2 of this paper deals with the literature survey and related work, section 3 with the proposed method of data embedding and data extraction Section 4 deals with experimental results followed by conclusion of the projectThe main aim of this paper is to improve the efficiency of the previously proposed method by increasing the embedding capacity per pixel and securely embedding more and various digital media data in a cover image.

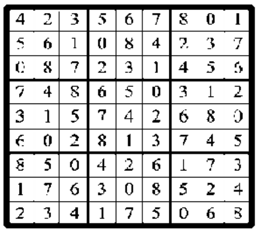
2. RELATED WORK

In this section, we will briefly describe steganographic scheme based on Sudoku solutions [7]. The central idea of this method is to modify the selected pixel pairs in the cover image which is 24-bit BMP using reference matrix. The secret data is converted to Base-9 for mapping them onto Sudoku solution. Sudoku solution is taken and every value in it is subtracted by '1' as shown in Figure 1&2. This is done so as to ensure all values lie between 0 and 8 in Sudoku, for maintaining compatibility between input data which is in Base-9 format. This Sudoku is then expanded to a 27 X 27 matrix called reference matrix (M) as shown in Figure 3.



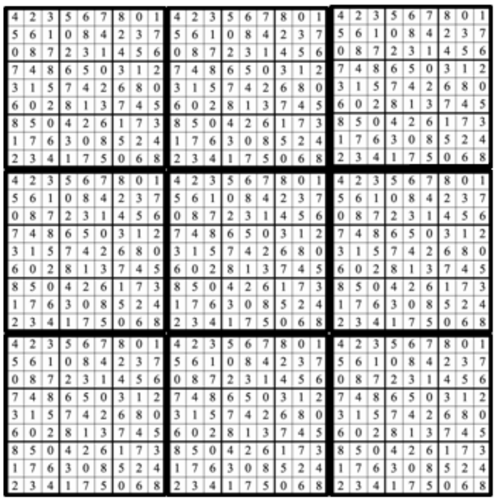
5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Figure 1: Sudoku solution



4	2	3	5	6	7	8	0	1
5	6	1	0	8	4	2	3	7
0	8	7	2	3	1	4	5	6
7	4	8	6	5	0	3	1	2
3	1	5	7	4	2	6	8	0
6	0	2	8	1	3	7	4	5
8	5	0	4	2	6	1	7	3
1	7	6	3	0	8	5	2	4
2	3	4	1	7	5	0	6	8

Figure 2: Reference Matrix



4	2	3	5	6	7	8	0	1	4	2	3	5	6	7	8	0	1	4	2	3	5	6	7	8	0	1
5	6	1	0	8	4	2	3	7	5	6	1	0	8	4	2	3	7	5	6	1	0	8	4	2	3	7
0	8	7	2	3	1	4	5	6	0	8	7	2	3	1	4	5	6	0	8	7	2	3	1	4	5	6
7	4	8	6	5	0	3	1	2	7	4	8	6	5	0	3	1	2	7	4	8	6	5	0	3	1	2
3	1	5	7	4	2	6	8	0	3	1	5	7	4	2	6	8	0	3	1	5	7	4	2	6	8	0
6	0	2	8	1	3	7	4	5	6	0	2	8	1	3	7	4	5	6	0	2	8	1	3	7	4	5
8	5	0	4	2	6	1	7	3	8	5	0	4	2	6	1	7	3	8	5	0	4	2	6	1	7	3
1	7	6	3	0	8	5	2	4	1	7	6	3	0	8	5	2	4	1	7	6	3	0	8	5	2	4
2	3	4	1	7	5	0	6	8	2	3	4	1	7	5	0	6	8	2	3	4	1	7	5	0	6	8
4	2	3	5	6	7	8	0	1	4	2	3	5	6	7	8	0	1	4	2	3	5	6	7	8	0	1
5	6	1	0	8	4	2	3	7	5	6	1	0	8	4	2	3	7	5	6	1	0	8	4	2	3	7
0	8	7	2	3	1	4	5	6	0	8	7	2	3	1	4	5	6	0	8	7	2	3	1	4	5	6
7	4	8	6	5	0	3	1	2	7	4	8	6	5	0	3	1	2	7	4	8	6	5	0	3	1	2
3	1	5	7	4	2	6	8	0	3	1	5	7	4	2	6	8	0	3	1	5	7	4	2	6	8	0
6	0	2	8	1	3	7	4	5	6	0	2	8	1	3	7	4	5	6	0	2	8	1	3	7	4	5
8	5	0	4	2	6	1	7	3	8	5	0	4	2	6	1	7	3	8	5	0	4	2	6	1	7	3
1	7	6	3	0	8	5	2	4	1	7	6	3	0	8	5	2	4	1	7	6	3	0	8	5	2	4
2	3	4	1	7	5	0	6	8	2	3	4	1	7	5	0	6	8	2	3	4	1	7	5	0	6	8
4	2	3	5	6	7	8	0	1	4	2	3	5	6	7	8	0	1	4	2	3	5	6	7	8	0	1
5	6	1	0	8	4	2	3	7	5	6	1	0	8	4	2	3	7	5	6	1	0	8	4	2	3	7
0	8	7	2	3	1	4	5	6	0	8	7	2	3	1	4	5	6	0	8	7	2	3	1	4	5	6
7	4	8	6	5	0	3	1	2	7	4	8	6	5	0	3	1	2	7	4	8	6	5	0	3	1	2
3	1	5	7	4	2	6	8	0	3	1	5	7	4	2	6	8	0	3	1	5	7	4	2	6	8	0
6	0	2	8	1	3	7	4	5	6	0	2	8	1	3	7	4	5	6	0	2	8	1	3	7	4	5
8	5	0	4	2	6	1	7	3	8	5	0	4	2	6	1	7	3	8	5	0	4	2	6	1	7	3
1	7	6	3	0	8	5	2	4	1	7	6	3	0	8	5	2	4	1	7	6	3	0	8	5	2	4
2	3	4	1	7	5	0	6	8	2	3	4	1	7	5	0	6	8	2	3	4	1	7	5	0	6	8

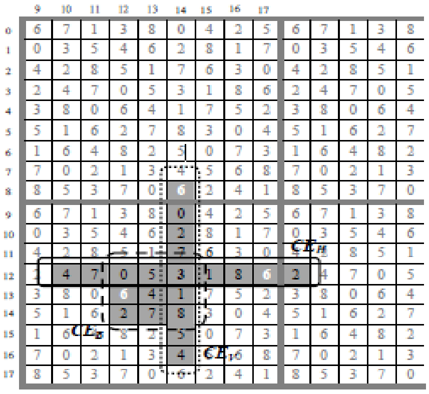
Figure 3: Reference Matrix of Order 27x27

2.1 Data embedding

In the data embedding phase, first convert the secret bit stream into secret digits in the base-9 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 $s_k \in [0, 8]$, $1\leq k\leq n$. Each pixel of this image is extracted and two components of pixel: Red (R) and Green (G) color are chosen for embedding. Each color component is an 8 bit binary number. The 8 bits represent numbers ranging from 0 to 255. This value is converted to a value between 0 and 8 using the following formula:

$$R = R \% 9, G = G \% 9$$

To this value of R and G, 9 are added for ensuring its value is located at the center of the reference matrix. Then R and G are chosen as X-axis and Y-axis components of reference matrix M, forming pair (g_i, g_{i+1}), where g =R and g_{i+1}= G. Then three candidate elements are chosen called Horizontal (CE_H), Vertical (CE_V) and Boxed (CE_B) all of which contains 9 elements. Here CE_H is shown by thick line, CE_V is shown by dotted line and CE_B is shown by dashed lines in Figure 4.



	9	10	11	12	13	14	15	16	17					
0	6	7	1	3	8	0	4	2	5	6	7	1	3	8
1	0	3	5	4	6	2	8	1	7	0	3	5	4	6
2	4	2	8	5	1	7	6	3	0	4	2	8	5	1
3	2	4	7	0	5	3	1	8	6	2	4	7	0	5
4	3	8	0	6	4	1	7	5	2	3	8	0	6	4
5	5	1	6	2	7	8	3	0	4	5	1	6	2	7
6	1	6	4	8	2	5	0	7	3	1	6	4	8	2
7	7	0	2	1	3	4	5	6	8	7	0	2	1	3
8	8	5	3	7	0	6	2	4	1	8	5	3	7	0
9	6	7	1	3	8	0	4	2	5	6	7	1	3	8
10	0	3	5	4	6	2	8	1	7	0	3	5	4	6
11	4	2	8	5	1	7	6	3	0	4	2	8	5	1
12	2	4	7	0	5	3	1	8	6	2	4	7	0	5
13	3	8	0	6	4	1	7	5	2	3	8	0	6	4
14	5	1	6	2	7	8	3	0	4	5	1	6	2	7
15	1	6	4	8	2	5	0	7	3	1	6	4	8	2
16	7	0	2	1	3	4	[illegible]	6	8	7	0	2	1	3
17	8	5	3	7	0	6	2	4	1	8	5	3	7	0

Figure 4: CE_H (Thick line), CE_V (Dotted line), CE_B (Dashed line)

The cover pixel pair (gi, gi+1) is modified as (gi1, gi+11) by a minimum distortion candidate element M (xmin, ymin) which is selected by using Manhattan distance formula:

$$M (xmin, ymin) = minj =H, V, B \{| gi – xj | + | gi+1 – yj|\}$$

Thus, the cover pixel pair (gi, gi+1) is modified as (gi1 = xmin, gi1+11 = ymin) to conceal the secret digit Si with small distortion.

2.2 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). Their pixel values are taken and converted to a value between 0 and 8 using the following formula:

$$R = R \% 9, G = G \% 9$$

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-9) is converted to base-2.

3. PROPOSED METHOD

Steganography using Sudoku is used to hide data or secret information onto an image using Sudoku solution. The image used in our proposed method is a 24 bit colored image. Initially the data to be hidden is chosen which can be any digital media file such as text, image, audio, video etc. Sudoku solution is taken and every value in it is subtracted by '1'. This is done so as to ensure all values lie between 0 and 8 in Sudoku so as to maintain compatibility between Sudoku and secret data which is a three bit value from the input data. 9x9 Sudoku is used as reference matrix M for both data embedding and extraction. Before embedding, one or more media files are compressed and encrypted to increase the efficiency and security of the method. DES technique is used for encrypting.

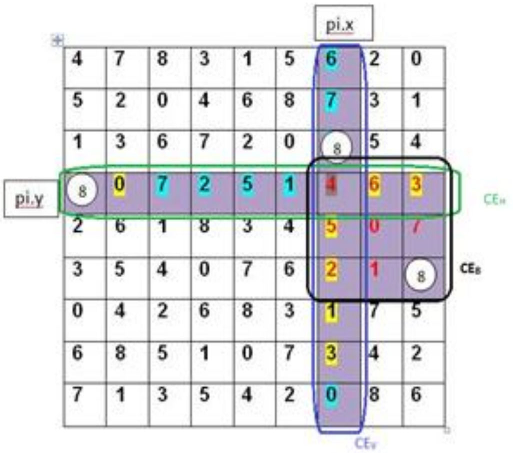
3.1 Data embedding

Any image onto which secret data has to be embedded is chosen. Two pixels of this image are chosen and RGB values of both the pixels are paired as C1(R1,G1), C2(B1, R2), C3(G2, B2) we can generalize each pair as Ci(x, y). For each pair

$$Pi.x =Ci.x \% 9, pi.y = Ci.y \% 9$$

Then Pi.x and Pi.y are chosen as X-axis and Y-axis components of reference matrix M. Then three candidate elements Horizontal (CE_H), Vertical (CE_V) and Boxed (CE_B) are chosen. Here CE_H is shown by green line, $CE_{V\ s}$is shown by purple line and CE_B is shown by black square in Figure 5. CE_H and CE_B are chosen so that M (Pi.x, Pi.y) from M is put in middle position of the candidate element array. The remaining positions are filled by respective left and right elements from position of M (Pi.x, Pi.y) in reference matrix. The difference in index positions of secret digit and M (Pi.x, Pi.y) is always less than or equal to 4 reducing the distortion in cover image.

```
Initialization of CE_H:
For (i: 0 to 8)
        pos = (i+4) %9
        CE_H [pos] = M (Pi.x, Pi.y)
        Pi.x = (Pi.x+1) %9
End For
Initialization of CE_V:
For (i: 0 to 8)
        pos = (i+4) %9
        CE_V [pos] = M (Pi.x, Pi.y)
        Pi.y = (Pi.y+1) %9
End for
```



4	7	8	3	1	5	6	2	0
5	2	0	4	6	8	7	3	1
1	3	6	7	2	0	8	5	4
8	0	7	2	5	1	4	6	3
2	6	1	8	3	4	5	0	7
3	5	4	0	7	6	2	1	8
0	4	2	6	8	3	1	7	5
6	8	5	1	0	7	3	4	2
7	1	3	5	4	2	0	8	6

Figure 5: Illustration of CE_H (green line), CE_V (purple line), CE_B (black square)

Pi.x = Ci.x%9
Pi.y = Ci.y%9

```
Initialization of $CE_B$:
For (i: 0 to 2)
    For (j: 0 to 2)
            posx = |_ Pi.x/3_|*3
            posy = |_ Pi.y/3_|*3
           $CE_B$ [posx] [posy] = M (Pi.x, Pi.y)
            posx++
    End for
   posy++
End for
```

Selecting optimum modified pixel value:

```
Positional Difference between Si and M (Pi.x, Pi.y) in $CE_H$
Find the position of Si in $CE_H$ say it as pos.
DH=pos-4
Positional Difference between Si and M (Pi.x, Pi.y) in $CE_V$
Find the position of Si in $CE_V$ say it as pos.
DV=pos-4

Find the position of Si in $CE_B$ say it as posx and posy.
SQX=posx-(Pi.x%3)
SQY=posy-(Pi.y%3)
SQD=|SQX|+|SQY|
```

The minimum distance is calculated by,

```
Min=minimum (|DH|, |DV|, SQD)
If min =|SQD| Ci.x = Ci.x + SQX
                    Ci.y = Ci.y + SQY
Else If min=|DH| Ci.x= Ci.x+ DH
Else min=|DV| Ci.y =Ci.y + DV

If Ci.x<0 Ci.x=9+Ci.x or Ci.x>255 Ci.x=Ci.x-9.
If Ci.y<0 Ci.y=9+Ci.y or Ci.y>255 Ci.y=Ci.x-9.
```

As in above Fig 5 Pi.x=6, Pi.y=3, so M (Pi.x, Pi.y) = 4 and Si=8.The candidates elements are selected as

CE_H= {7, 2, 5, 1, 4, 6, 3, 8, 0},
CE_V= {0, 6, 7, 8, 4, 5, 2, 1, 3},
CE_B={{4,6,3},{5,0,7},{2,1,8}}.

Here DH=7-4=3, DV=3-4= -1,
SQX=8-6=2 & SQY=5-3=2.
SQD=SQX+SQY=2+2=4.

Min=minimum{|DH|,|DV|,|SQD|}=minimum{3,1,4}=1,So Ci.x=Ci.x Ci.y=Ci.x+DV.

As a result 9 bits are embedded in two pixels. Similarly apply above method for C2 & C3. The above method ensures the each component of pixel is modified maximum by 4 when its value is greater than 3 and less than 252. Repeat the above procedure until the data gets embedded in cover image, if cover image is not big enough to hold all the data then new cover image should be used until all the data is embedded. Figure 6 shows images before embedding and after embedding.

The first 10 pixels of cover image are reserved to embed the size of input data file which is a zip file consisting of variable input media data files. If a cover image can't embed all input data file then remaining data is embedded in new images until all the data is embedded. Sudoku solution is encrypted and then it is embedded using the LSB method in which 3 bits of encrypted Sudoku is embedded so that each bit is at least significant bit of R, G, and B component of cover image pixel.

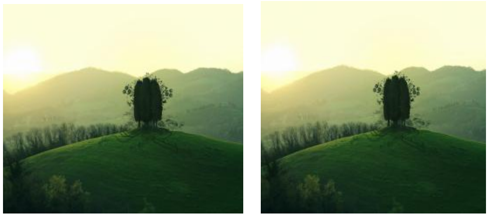


Figure 6.a) Cover Image b) Stego Image

3.2 Data extraction

Two pixels of this image are chosen and RGB values of both the pixels are paired as C1 (R1, G1), C2 (B1, R2), C3 (G2, B2) we can generalize each pair as Ci(x, y). For each pair

Pi.x =Ci.x % 9, Pi.y = Ci.y % 9

Then Pi.x and Pi.y are chosen as X-axis and Y-axis of reference matrix M. M (Pi.x, Pi.y) is secret data extracted. This process is repeated for C1 and C2 pairs .Then again the whole process is repeated till the required size of secret data is retrieved which is obtained from extracting ten pixels of first cover image.

Encrypted Sudoku solution from the received cover image is extracted from LSB of R, G and B components of cover image. The pixels from cover image are used for extraction until size of encrypted Sudoku is obtained which is embedded in cover image. Sudoku solution is retrieved by decrypting Encrypted Sudoku.

4. EXPERIMENTAL RESULTS

While designing image steganography main factors to be considered are:

1) Embedding more data securely in a cover image.

2) Number bits to be embedded per pixel.

3) Less distortion in embedded cover image compared to

original cover image.

In our proposed system first condition is met by using compression technique specific to input media files and encryption for secure exchange resulting in less data to embed as shown in Table 1.

Table 1. Compression of data

Input data	Compressed data
Sample1.pdf-297KB	Compressed File. Zip -1.84MB
Sample2.png-198KB	
Sample3.mp3-.53MB	
Totalsize-2.01MB	

So, the total number of bytes to be embedded is always less in this method compared to method [7].

The number of bits embedded per pixel is 4.5 bits which is 1.5 bits higher than the method [7].

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 to evaluate the quality of an image. The PSNR is defined as follows

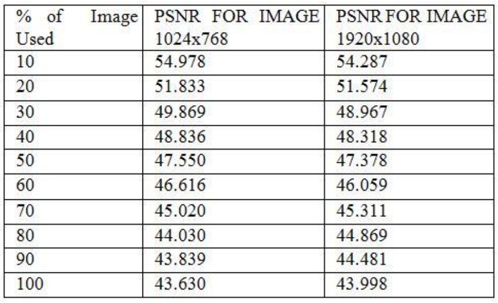
$$\mathrm{PSNR} = 10 \cdot \log_{10} \frac{255^2}{\mathrm{MSE}} \text{ dB},$$

where MSE is the mean square error between the original image and the stego image. The MSE is defined as follows:

$$\mathrm{MSE}= \frac{1}{3 \text{ X } M \text{ X } N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1}(R_{ij} - R_{ij}^{|})^2+\sum(G_{ij} - G_{ij}^{|})^{2+}\sum(B_{ij} - B_{ij}^{|})^2$$

where R_{ij},G_{ij},B_{ij} nd $R_{ij}^{|}$,$G_{ij}^{|}$,$B_{ij}^{|}$ are RGB value of orginal and stego images pixels respectively. M X N gives number of all pixel present in a image. A larger PSNR indicates that the quality of the stego image is closer to the original one. Normally human's eyes find it hard to distinguish between the distortions on a stego image compared to original image when its PSNR value is greater than 30 dB.The PSNR values given by our system for variable percentage of pixels used for embedding for different cover images of resolution 1024x768 and 1920x1080 are shown in Table 2 and respectively in bar chart in Fig.7. So if all the pixels of both original cover images are used for embedding then value of PNSR is equal to 43.63 and 43.998 respectively, which is higher than threshold value (30dB). However PSNR values are lesser by 5dB when compared to method [7].

Table 2. Percentage of image used and PSNR values for 1024x768 and 1920x1080 images.



% of Image Used	PSNR FOR IMAGE 1024x768	PSNR FOR IMAGE 1920x1080
10	54.978	54.287
20	51.833	51.574
30	49.869	48.967
40	48.836	48.318
50	47.550	47.378
60	46.616	46.059
70	45.020	45.311
80	44.030	44.869
90	43.839	44.481
100	43.630	43.998

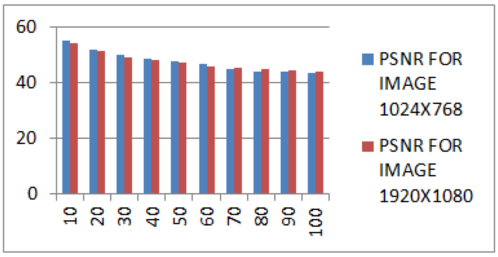


Figure 7: Graph showing relation between PSNR along Y-axis and percentage of image used for data embedding along X-axis

5. CONCLUSION

In this paper we have proposed the revised version of [7]. In earlier work only the RED & GREEN components of cover image pixel were used. So embedding capacity was 3 bits per pixel and reference matrix used was of order 27 X 27. 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 (CE_H, CE_V, CE_B) are chosen in such way that less distortion is produced in cover image after embedding the data. In previous system 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. System provides two layer security one by using a random Sudoku among 6.671×10^{21} possible solutions and other by using strong encryption algorithm. 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. Stego image generated holds more data and is less distorted compared to other proposed system. Stego images are in lossless format and less space for stego images can be obtained if this method is extended for stego images in loss format.

6. ACKNOWLEDGEMENT

The authors acknowledge and thank the support of Dr. N.K.Srinath, Head of Dept of Computer Science and Engineering, R. V. College of Engineering and Assistant Prof Ms.Usha B A for their constant support and guidance.

7. REFERENCES

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

[2] C.-C. Chang and C.-Y. Lin. Reversible steganography for vq- compressed images using side matching and relocation. *IEEE Transactions on Information Forensics and Security*, 1(4):493–501, 2006.

[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] Yung-Chen Chou, Chih-Hung Lin, Pao-Ching Li, Yu-Chiang Li A (2, 3) Threshold Secret Sharing Scheme Using Sudoku 2010 *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* 978-0-7695-4222-5/10, 2010

[5] 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.

[6] Wien Hong, Tung-Shou Chen, Chih-Wei Shiu, Steganography Using Sudoku Revisited *Second International Symposium on Intelligent Information Technology Application* 978-0-7695-3497-8/08, 2008

[7] Roshan Shetty B R, Rohith J, Mukund V, Rohan Honwade Steganography using Sudoku Puzzle, 2009 *International Conference on Advances in Recent Technologies in Communication and Computing* 978-0-7695-3845-7/09, 2009