Wireless Personal Communications (2022) 127:979–995
https://doi.org/10.1007/s11277-021-08477-1

An Approach for Attaining Content Confidentiality on Medical Images Through Image Encryption with Steganography

R. Bala Krishnan[1] · N. Rajesh Kumar[1] · N. R. Raajan[2] · G. Manikandan[3] · A. Srinivasan[4] · D. Narasimhan[5]

Accepted: 13 April 2021 / Published online: 22 April 2021

Abstract
The process of content confidentiality of the medical diagnostic reports and the scanned image of patients among doctors with balancing proficiency for mutual dealing will provide utmost care through faster and significant decisions. The medical field's present-day technology with information technology has made it possible to deliver and distribute digital information in a more comfortable way at a faster rate. This simpleness of the content makes the issue of exhibiting the transmitted digital content on the network with the chance of illegal interception. Traditional cryptographic mechanisms follow the trend of encrypting the content before transmission to improve content confidentiality. However, the encrypted information's visual aspect makes the intruder focus more on the range, leading to malicious attacks. Hence the routine of data hiding has received substantial aid as an alternative way to ensure information security. This paper presents a biomedical data concealment procedure with Sudoku based scrambling on Biomedical DICOM image and Queen Traversal pattern for locating the pels over the DICOM image. It hides the confidential medical data in the scrambled or encrypted cover images. Experimental outcomes establish the efficacy of the system viz-a-viz respective parameters of interest.

Keywords Queen tour · Biomedical images · DICOM · Content concealment · LSB embedding · Secret data · Scrambling

1 Introduction

Information security focuses on strengthening private content, but the field has been developed with the most recent digital communication discipline maturation. The terminologies 'Crypto' and 'Stego' are two substantial proficiencies used for data transformation and content concealment on standard and biomedical images [1]. The proficiency Steganography pretends a vital role in hiding confidential information through data hiding techniques. It can be achieved by storing the secret code in digital images, audio, or video files so that

✉ G. Manikandan
manikandan@it.sastra.edu

Extended author information available on the last page of the article intruders do not estimate the secret code's existence [2, 3]. The practice of covering the secret code in a digital medium such as files, images, audio, or video files is referred to as the "Content Embedding" operation [4–6].

The development of Steganography makes it a robust mechanism to protect secret code, especially the data of telesurgery, telediagnosis, and tele-consulting over the network channel. The advancement of this content concealment practice leads to image analysis (steganalysis) schemes [7, 8] that are similar for all the content concealment [9, 10] schemes. Several methods of stego principles are introduced [11–13] and are grouped into two significant cases based on their domain of the cover (input) images, which are spatial [14–16] and frequency [17–19]. In the spatial domain, the encrypted secret code is concealed in the pels of the input image by applying Least Significant Bit substitution [20–22], run-length [14, 23], PVD [24], reversible [12, 15], mod [25] and lossless schemes for data hiding. In the frequency domain, the secret content is stored in the input image's transformed coefficients using the domain converters such as DCT and DWT [26, 27]. In the LSB procedure, random and raster scan schemes are implemented to hide the secret code over the image pels. The random scan is preferred more than the raster scan because of its content extraction complexity.

An Optimal Pixel Adjustment Process (OPAP) to increase the content embedded Image's value by simple LSB substitution method is stated by Chan et al. [4]. The count of bits to be embedded on each of the image pels would get decided by the adjustment strategy. As a result, it cumulates merely the count based on the neighboring pels. An LSB substitution strategy using the raster scan method to improve stego-image is stated by Yang et al. [22]. The secret code has been processed before the content concealment process. Another embedding procedure using the Bishop Tour scheme of the chess game is stated by Bala Krishnan et al. [28], in which the content embodiment could be achieved by following the black and white bishop tour principle. A random way to select the Image pels for secret code embedding has been proposed by Provos et al. [17]. Another content embedding practice using random fashion has been stated by Tuomas Aura [23], which follows the SHA and stego fundamental principles to produce a series of unique pel locations over the Image for content concealment. Another LSB with Queen tour of chess game-based embedding scheme is stated by Manikandan et al. [29], which offers content embedding by following Queen placement pattern in a 8 × 8 chessboard. All the existing information hiding principles focused only on the pixel accessing order on the cover image [4]. There is no focus on the implementation of cryptographic implementation on cover images before the secret content embodiment process, which would be a significant limitation on the existing principles [13, 17, 25, 29].

The authors of the proposed model offer and exhibit a novel approach of secret content embodiment in the scrambled DICOM images in this anticipated work. For pels identification, the Queen Traversal pattern of the chess game is followed. The result has been enforced to attain massive complexity and a higher payload during the illegal content extraction. The cover DICOM image has been partitioned into an equal number of smaller blocks, subjected to the scrambling process by following the Sudoku pattern. During the secret medical data embedding practice, the tour patterns have been implemented to locate the Image's pels. The LSB substitution scheme embeds the secret content and the final descrambling results in the DICOM stego image. This proposed system's implementation results in the least Means Square Error (MSE) and maximum Peak Signal to Noise Ratio (PSNR) value for the stego DICOM images. The best traversal pattern for locating the pels and Image scrambling and descrambling patterns is kept as the key (secret) for content extraction.

2 Related Work

A variety of techniques has also been suggested on Steganography and Sudoku solver over the past. The methods are followed for information concealment on digital images, which grant lossless image compression.

2.1 Sudoku Pattern for Image Scrambling

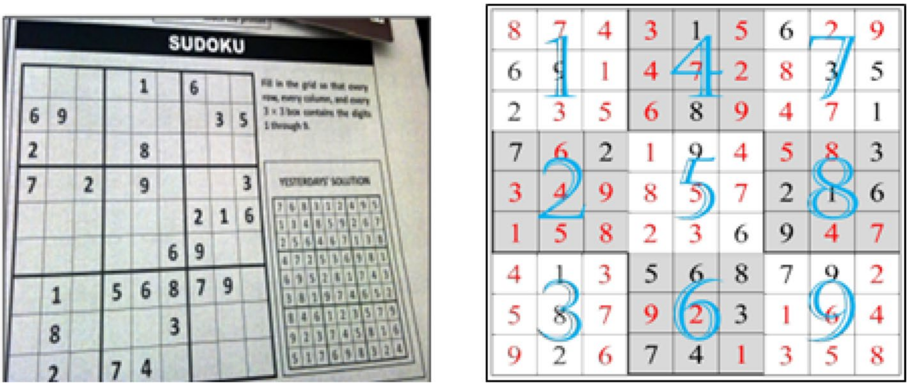
An efficient image scrambling approach using Sudoku pattern and Latin squares is presented by Wu et al. and Zhang et al. [30–32]. The scrambling principle performs Image scrambling through Shuffling and Sudoku patterns, and it offers the reverse of the Sudoku and Shuffling pattern for image reconstruction. The term ‘Sudoku’ is the abbreviation of ‘Sunji wa dokushin ni kagiru’ from the Japanese language. The technique Sudoku refers to a puzzle based on numbers; generally, it contains a grid with 9×9. The grid is then separated into nine 3×3 sub-blocks. The Sudoku solver’s theme is to arrange the grids using digits ranging from 1 to 9, in the behavior that there are no repetitive digits in any single column, row, and block of the whole puzzle. A sample puzzle of Sudoku and its solved result is stated in Fig. 1.

2.1.1 Sudoku Matrix Definition

A ‘M × M’ matrix is a Sudoku matrix (SM) if its elements satisfy all three constraints that matrix elements in any row and any column, and in any m × m block contains exact M digits from 1 to M.

A Sudoku matrix of order ‘M × M’ satisfying the definition of SM has the properties together with, but not restricted to the states listed below.

- The ‘M’ elements within each row, column, and block of the matrix (Sudoku puzzle) is a permutation of the natural number sequence {1, 2, … M}



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

(a) Sudoku question

(b) Result for Sudoku question

Fig. 1 Sudoku question and its result. **a** Sudoku question, and **b** solved Sudoku puzzle

A subset of ‘MxM’ matrices of the Sudoku puzzle can be generated perimetrically [33]. It is noticeable that the above stated three properties are directly taken from the description of a Sudoku matrix.

The authors Hemanth et al. [34] presented a new approach to enhancing image steganography systems through the transforms domain. An approach for secret content embedding through contours has been presented by the authors Manikandan et al. [35]. The steganography principle on video has been presented by the authors Manisha et al. [36], in which the authors presented a two-level security model for secret data hiding process on videos. The authors Ansari et al. [37] presented a comparative study model for utilizing various steganography applications. Another approach stated by the authors Manikandan et al. [38] to hide Image over images. The above-stated model embeds the Image on another image, and at the receiver end, the embedded Image could be extracted without loss. An approach of Steganography using fractal set has been stated by Mohammad Alia et al. [39]. It offers an improved steganography model for the embodiment of secret content on digital images.

3 Proposed Methodology and Its Implementation

For implementing the proposed Queen Tour Based Content Embedding (QTBCE) technique, five different images with resolution ‘lxm’ have been taken as inputs, where l = m for a square image and l = m = 1200. As for implementing the proposed model, the image dimension’s value has been considered 1200 × 1200, with a resolution of 300 dpi. The input cover images are stated in Fig. 2i–v.

The proposed technique starts with the image segmentation process, in which the whole image is sub-divided into blocks of equal size for the scrambling process. The scrambling process works on the principle of the Sudoku game. The block diagram of the proposed QTBCE scheme is stated in Fig. 3.

The cover image ‘ci’ used for content concealment is enciphered using an encryption key. The Sudoku based scrambling process is to be followed for the enciphering principle because of its minimal computational complexity and efficiency. The execution pattern of the proposed methodology is stated in Sect. 3.3.

The scrambled Image has been broken into unique size blocks over 8 × 8 for the content concealment process and shown in Fig. 4. The concealment’s secret code has been divided into three variable-length data vectors: SC1, SC2, and SC3, to distribute the channels’ secret code. The relation between the data vectors is SC1 = TL/8, SC2 = (3 × TL)/8, and SC3 = TL/2, where TL is the secret code’s length embedding process.

The secret content (i.e.) the medical history of the patient is subjected to the concealment process. It is performed by locating the pels in the image channels. The pels selection

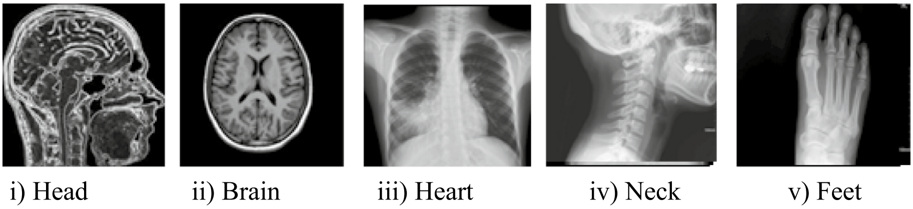


Fig. 2 Cover images for QTBCE scheme: **i** head, **ii** brain, **iii** heart, **iv** neck, and **v** feet

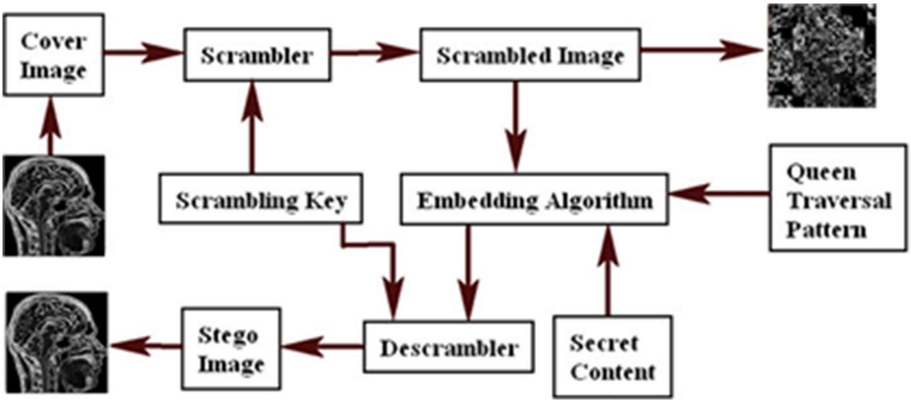


Fig. 3 Proposed queen tour based content embedding (QTBCE) system

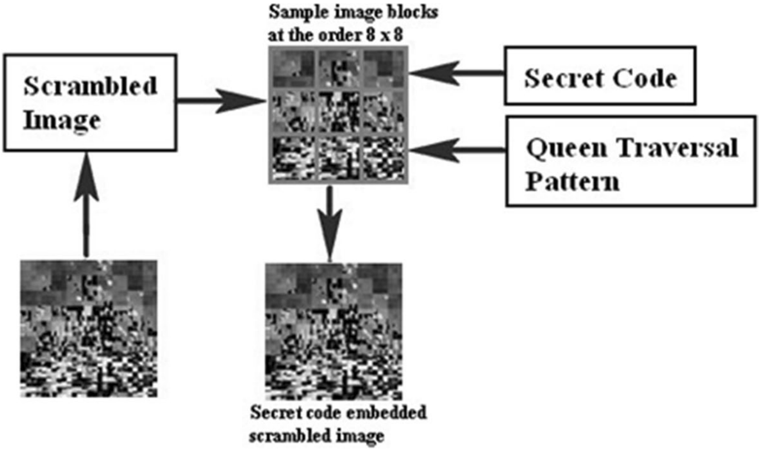

Sample image blocks at the order 8 x 8
Scrambled Image
Secret Code
Queen Traversal Pattern
Secret code embedded scrambled image

Fig. 4 The procedure of secret code concealment in a scrambled image

process follows the Queen Traversal of Chess game principle in 8×8 block, and the procedure is stated in Fig. 5. The Least Significant Bit (LSB) substitution procedure embeds the secret code in the image blocks.

The secret code gets embedded in all the image channels, such as red, green, and blue. The data vector SC1 gets embedded in the red channel blocks, SC2 in the green channel blocks, and SC3 on the blue channel blocks and the principle is stated in Fig. 6.

The content embodiment in all the blocks follows the Queen Traversal principle, as stated in Fig. 5. As per the scheme, the 8×8 block contains 8 non-attacking queens. There may be multiple choices for placing the non-attacking queen in the 8×8 chess game block. In our proposed scheme, the non-attacking queens' location is "8d 7f 6h 5b 4g 3a 2c 1e". The first queen's placement in the location "8d" offers four locations, namely "8e–8f–8g–8h" for the content embodiment, and through this queen placement, 8-bits of data gets embedded. The eight queens offer '28' locations for the content embodiment, which supports '56' bits of content embodiment in a single block. Table 1 shows the

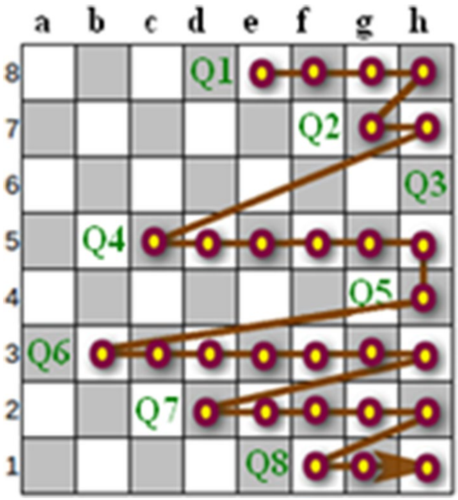


Fig. 5 Pel accessing order of queen traversal

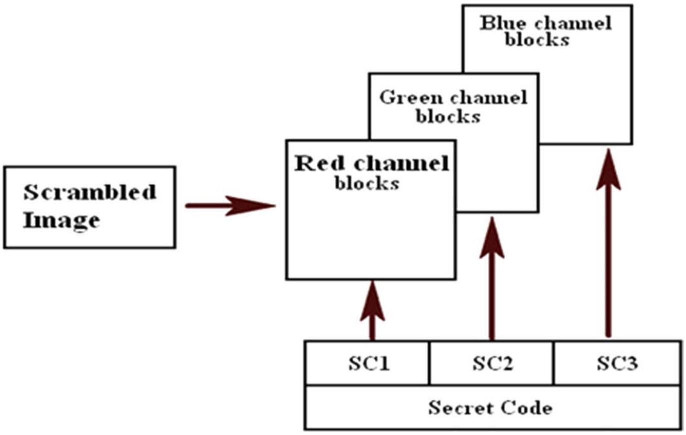


Fig. 6 Color channels and their corresponding secret code streams

Table 1 Queen placement and its corresponding locations for the data embedding process

Queen	Location	Locations for embedding	Bits capacity
Q1	8d	8e–8f–8 g–8 h	8
Q2	7f	7 g–7 h	4
Q3	6h	–	0
Q4	5b	5c–5d–5e–5f–5 g–5 h	12
Q5	4g	4 h	2
Q6	3a	3b–3c–3d–3e–3f–3 g–3 h	14
Q7	2c	2d–2e–2f–2 g–2 h	10
Q8	1e	1f–1 g–1 h	6

locations of the 8-queens in an 8 × 8 chess block and its corresponding areas for the content embodiment process.

3.1 Algorithm for Queen Traversal Based Secret Code Substitution Process in the Color Image

Inputs

1. Secret Content (SC) in bits
2. Cover Image
3. Scrambling Key (SK)
4. Queen Traversal Pattern

Output

1. Stego Image (SI)

Algorithm

```
Step 1: Identify the Secret Content (SC) for embedding.
Step 2: Calculate the length of the secret content (TL) in bits.
Step 3: Locate the Cover image and Queen Traversal pattern.
Step 4: Fragment the Cover Image (CI) into ‘x’ equal size blocks (CI_1, CI_2, …. CI_x)
Step 5: Identify the Sudoku Pattern ‘SK’ for the scrambling process.
Step 6: Apply the SK on the image blocks to obtain the Scrambled/encrypted image ‘EI’.
Step 7: Create data vectors SC1, SC2, and SC3 from SC and TL
            where  SC1 = TL/8
                   SC2 = 3(TL)/8 and
                   SC3 = TL/2
Step 8: Apply the Queen Traversal pattern to embed data in the Scrambled image EI.
```

The content from SC1 gets embedded in EI’s red channel, content from SC2 gets embedded in the green channel of EI, and SC3 on the blue track of EI.

Step 9: Apply the descrambling process in the EI to obtain the Stego Image ‘SI.’

3.2 Algorithm for Queen Traversal Based Secret Code Extraction Process in Color Image Inputs

1. Stego Image (SI) containing the embedded Secret Content (SC)
2. Scrambling Key
3. Queen Traversal (QT) Pattern
4. Length of the Data Vectors SC1, SC2, and SC3 and store it in L1, L2, and L3

Output
Secret code stream of length (TL) in bits.

Algorithm

Step 1: Fragment the stego image (SI) into ‘x’ equal size blocks (SI_1, SI_2, …. SI_x)

Step 2: Identify the Sudoku Pattern key or scrambling key for the scrambling process

Step 3: Apply the Sudoku pattern on the image blocks to obtain the Scrambled stego image ‘SSI.’

Step 4: Apply QT pattern to locate the pels accessing path in the scrambled stego image SSI.

Step 5: Extract content from the LSB positions in all the channels of the Image.

Extract L1 bits from red channel,

L2 bits from the green and

L3 bits from the blue channel.

Step 6: Concatenate the extracted L1, L2, and L3 bits and store them in SC

Step 7: Display the SC.

3.3 Execution of the Proposed Methodology

The proposed scheme’s execution procedure is stated in Fig. 3, and the workflow of the scrambling and embedding process is presented in Sect. 3.1 algorithmically. The cover image is forwarded to the scrambler to generate the encrypted Image. For the procedure, the Image could be sub-divided into blocks of the same size. A systematic and efficient process of blocks could be performed to generate the encrypted Image. The procedure for the encrypted or scrambled image generation could be the Sudoku technique. For the Sudoku-based scrambling process, the sub-divided blocks are subjected to the assignment of unique numbers, and by following the Sudoku pattern, the numbered blocks are then rearranged; as a result, an efficient scrambled or encrypted image has been obtained.

All the stego principles implement the content concealment process over the cover image only. The proposed scheme offers an efficient multilevel security platform over the secret content by storing the secret content on an encrypted image. The content concealment process offers a proficient traversal scheme for locating the pels over the Image for the content embodiment process, and the Queen Traversal pattern is stated in Fig. 5. The secret content gets embedded in all the channels of the Image. The secret code gets subdivided into three data vectors for improving the level of confidentiality over the content. The existing content schemes hide the secret code sequentially, whereas the proposed system performs a data dividing scheme for separating the secret code. The codes are stored in the data vectors SC1, SC2, and SC3. The channel accessing procedure of the data vectors is stated in Fig. 6. The proposed scheme offers six different strategies for storing the contents over the Image, and the options are indicated in Table 2.

As per the mentioned schemes in Table 2, Scheme A hides the content of SC1 in the red channel, and SC2 and SC3 load the content in green and blue channels, respectively. In order to improve the chaotic level of content hiding, multiple schemes are proposed, and the order of the data vectors SC1, SC2, and SC3 are distorted in each of the methods for accessing the color channels. The content extraction process at the receiver end is stated in Sect. 3.2, and the procedure starts by scrambling the received Image. And in the scrambled

Table 2 Data vector schemes and their corresponding color channels

Color Channels	Scheme A	Scheme B	Scheme C	Scheme D	Scheme E	Scheme F
Red	SC1	SC2	SC3	SC1	SC2	SC3
Green	SC2	SC3	SC1	SC3	SC1	SC2
Blue	SC3	SC1	SC2	SC2	SC3	SC1

Image, the proposed queen traversal is applied for locating the pels. For the secret content extraction, the traditional LSB extraction could be followed in all the image color channels according to the schemes depicted in Table 2. The proposed model could be incorporated over the healthcare services domain to transfer the patient details effectively. The medical practitioner could utilize the proposed model to effectively share the patient details and the medical reports to other medical practitioners and the authorized recipients.

4 Experimental Observations

Process the digitized Image encompasses numerous metrics to quantify the image properties. The MSE and PSNR are such metrics applied to appraise the quality and error rate between the images. The former is almost inversely proportional to the latter. Other quantifying metrics such as compression ratio, content embedding, and extraction time also plays a vital role.

4.1 Mean Squared Error (MSE)

It is to identify the squares of the error between two images. Usually, it is a set of numerical values, and its computing equation is

$$\text{MSE (Color Image)} = \frac{1}{N^2}\sum_{\text{i=1}}^{\text{N}}\sum_{\text{j=1}}^{\text{N}}[\big(\text{R(i,j)} - \text{R}^{*}\text{(i,j)}\big)^2 + \big(\text{G(i,j)} - \text{G}^{*}\text{(i,j)}\big)^2 + \big(\text{B(i,j)} - \text{B}^{*}\text{(i,j)}\big)^2] \ldots \text{(e)}$$

where CImage and SImage represent the cover and stego image, respectively. The R(i, j), G(i, j), and B(i, j) denotes the pixels (Red, Green, and Blue) in locations(i, j) of the CImage, R′ (i, j), G′ (i, j) and B′ (i, j) represents the pixels of the SImage, and an N × N denotes the resolution of the images.

4.2 Peak Signal to Noise Ratio (PSNR)

The ratio between signal variance and reconstruction error variance is computed through the PSNR value, and it can be calculated through the following expression.

$$PSNR = 10\log_{10}\frac{255^2}{\text{MSE}}\text{(f)}$$

4.3 Content Embedding and Extraction Time

Any compression system uses one of the enciphering principles for generating the cipher code for the input content. The cipher generation practice is very crucial for the success of the system. It involves the representation of the input content in a form that is appropriate for storage and transmission. The time taken to accomplish this operation is denoted as embedding time, and the reverse is the extraction time. The proposed QTBCE approach has been implemented, and tests are conducted using the medical images shown in Fig. 2.

The proposed approach performs the content embedding process on the scrambled Image. For the content concealment, the Queen Traversal pattern could be followed for locating the pels over the Image's color channels. The input cover Image dimensions were 1200 × 1200; through this Image, 109,200-bits secret content has been taken for embedding practice. The experiments' outcomes are shown in Fig. 7, displaying the cover image and its corresponding scrambled Image without content concealment and the scrambled Image with secret content. After the content concealment process, the Image would be subjected to a descrambling process to obtain the stego image, which looks similar to the cover image.

The difference between the cover image and the stego image could be identified through the MSE and PSNR values. In the proposed approach, six distinct schemes for content embodiment are introduced and are stated in Table 2. The following Table 3 shows the cover and stego images' comparison outcomes, respectively, according to the schemes.

It is to be denoted that Table 3 shows the outcomes of the comparison of the stego image with its corresponding cover image. The MSE value states that the variation between the images is very low. The similarity between the images is at an acceptable rate, which is observed through the PSNR value. The comparisons between the proposed schemes (Scheme A to F) based on the observed PSNR values are presented in Fig. 8. The proposed QTBCE, besides furnishing a substantial betterment in procedures (A to F), offers an additional feature of multilayer security, as data embedding using the methods has been carried out by following Queen Traversal in the scrambled images, and the descrambling generates final stego image. This means an opponent must know the scrambling key for obtaining the scrambled Image besides knowing Queen Traversal and the schemes (Scheme A to F) pattern to get back the secret content from the stego image.

5 Significance of the Proposed Approach

The proposed QTBCE system applies three mechanisms for influencing content confidentiality. They are.

- Scrambling and De-scrambling of images (Image Encryption).
- Secret content substitution by Queen Traversal pattern for locating the pels.
- Secret content partitioning along with Schemes (A to F) for embedding the content in color channels.

All the traditional stego principles, the pels accessing order, hold the lock of secret content extraction. Still, the proposed system maintains the first lock at the image encryption technique, the second lock at the Queen Traversal based pels accessing order, and the final lock is the content extraction schemes.

6 Security Analysis

The proposed approach comprises the encryption principle on Image to obtain an enciphered image and Steganography principle for hiding a secret content in an enciphered image. The proficient footprints implied in the proposed system is

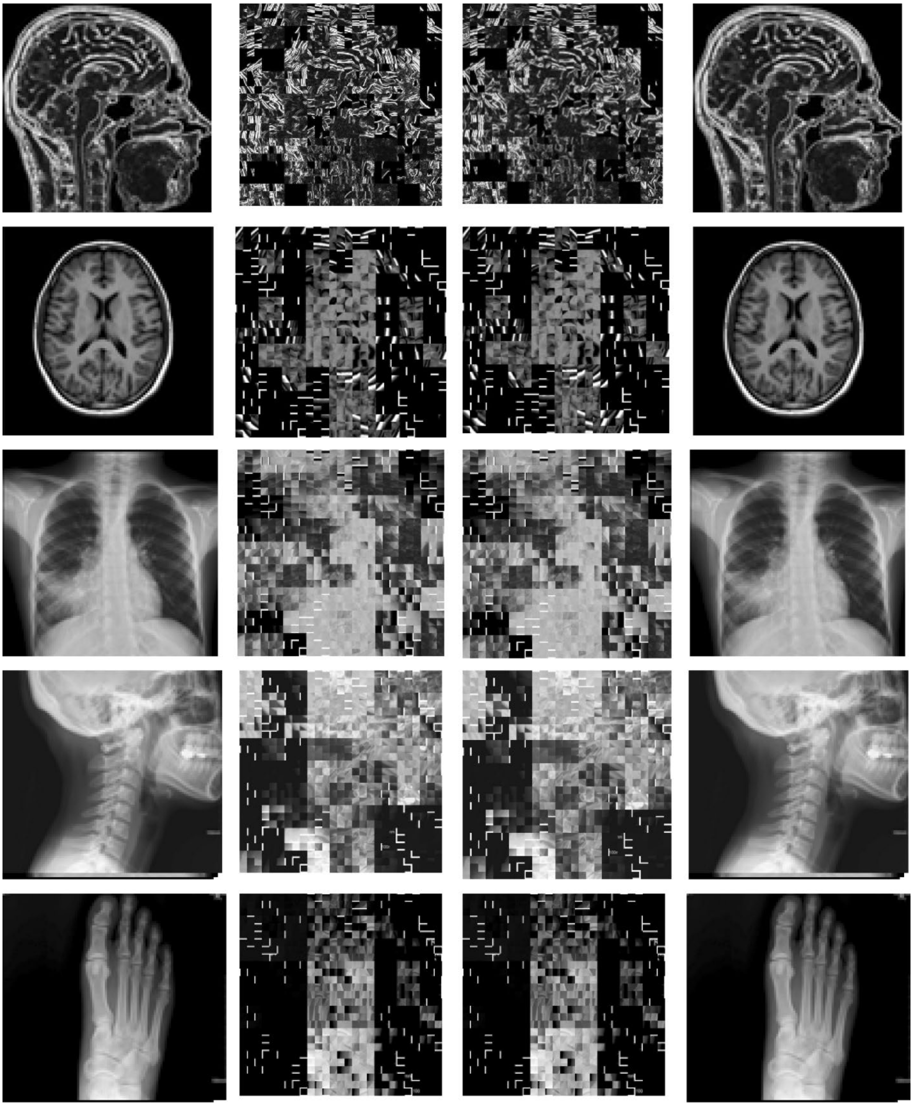


Fig. 7 Cover Image with its corresponding scrambled image and stego image

- The cover image gets reordered or scrambled by applying the Sudoku Pattern key.
- The secret content is partitioned into distinct size vectors, which are located for color channels.
- The Scrambled Image is subjected to LSB substitution by following the proposed Queen Traversal schemes.
- Descrambling on the content embedded Image would generate the final stego image.

The scrambling key and the traversal principle, and data vectors partitioning schemes are needed to get back the confidential medical data from the DICOM images at the

Table 3 Comparison of cover and stego images according to the schemes

Schemes	Cover image									
	Head		Brain		Heart		Neck		Feet	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Scheme A	0.00076	79.31096	0.00027	83.87633	0.00025	84.10597	0.00023	84.45359	0.00027	83.87633
Scheme B	0.00071	79.58914	0.00023	84.58324	0.00028	83.62292	0.00025	84.06684	0.00025	84.18529
Scheme C	0.00046	81.46130	0.00020	85.04569	0.00031	83.28478	0.00022	84.64955	0.00026	84.02807
Scheme D	0.00083	78.94631	0.00032	83.09385	0.00026	83.98963	0.00023	84.60523	0.00027	83.85773
Scheme E	0.00064	80.05235	0.00024	84.28653	0.00029	83.55315	0.00021	84.87817	0.00023	84.56136
Scheme F	0.00050	81.11168	0.00021	84.80831	0.00033	82.94091	0.00026	84.04741	0.00026	84.00881

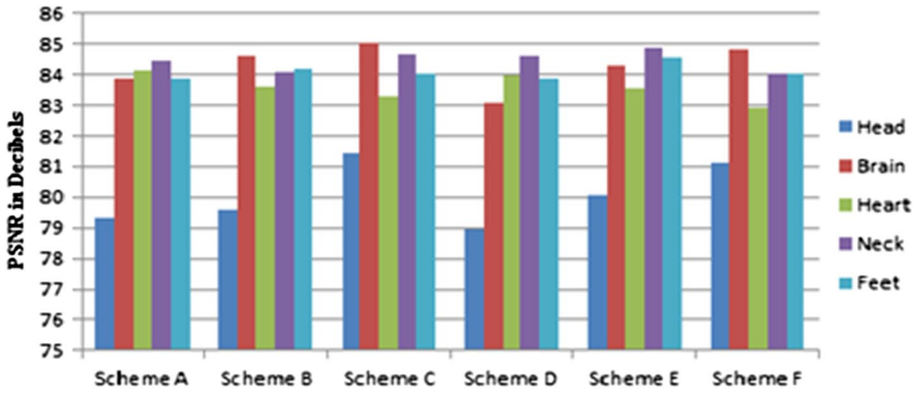


Fig. 8 Comparison of the proposed system schemes (A to F)

receiver end. Hence the proposed system offers a multilevel level of security to the confidential medical data of the patients.

7 Conclusions

An efficient approach with a high ability to accomplish the secured data hiding has been presented in this paper. The existing steganography models perform embodiment on the cover image alone, whereas the proposed model works with the scrambling and then embedding process. Initially, the cover image gets enciphered by applying a Sudoku based scrambling mechanism. The outcome of the scrambling would serve as a base for the content concealment process. The secret code gets partitioned into distinct data vectors for the embedding procedure and the Queen Traversal pattern for locating the pels over the image channels. The secret content embodiment is carried out in the encrypted Image. The Image is subjected to a descrambling process to obtain the stego image; the system offers a high protection level to the secret content without complexity. From the experimental observations, it is evident that the proposed scheme provides a good quality of stego images with multilevel security, which makes the system more suitable for convert communications. The implementation of traversal patterns on videos for data embodiment would be the future direction of this research work.

Funding Not applicable.

Conflicts of interest The authors declare that they have no conflict of interest.

References

1. Schneier, B. (2007). *Applied cryptography protocols* (2 ed.). Algorithm and source code in C. Wiley India Edition.

2. Bender, W., Butera, W., Gruhl, D., Hwang, R., Paiz, F. J., & Pogreb, S. (2000). Applications for data hiding. *IBM Systems Journal, 39*(3 & 4), 547–568
3. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal, 35*(3 & 4), 313–336
4. Chan, C. K., & Chen, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition, 37*(3), 469–474
5. Narayanan, P., Sengan, S., Pudhupalayam Marimuthu, B., et al. (2021). Analysis and design of fuzzy-based manoeuvring model for mid-vehicle collision avoidance system. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02737-x
6. Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information hiding techniques for steganography and digital watermarking*. Norwood, MA: Artech House.
7. Liu, Q., Sung, A. H., Qiao, M., Chen, Z., & Ribeiro, B. (2010). An improved approach to steganalysis of JPEG images. *Information Sciences, 180*, 1643–1655
8. Zhang, T., Li, W., Zhang, Y., Zheng, E., & Ping, X. (2010). Steganalysis of LSB matching based on statistical modeling of pixel difference distributions. *Information Sciences, 180*, 4685–4694
9. Westfeld, A. (2005). Space-filling curves in steganalysis. In: E. J. Delp, III, & P. W. Wong (Eds.), Security, steganography and watermarking of multimedia contents VII SPIE 5681 (pp. 28–37).
10. Luo, X.-Y., Wang, D.-S., Wang, P., & Liu, F.-L. (2008). A review on blind detection for image steganography. *Signal Processing, 88*, 2138–2157
11. Chang, C.-C., Wen-Chuan, Wu., & Chen, Y.-H. (2008). Joint coding and embedding techniques for multimedia images. *Information Sciences, 178*(18), 3543–3556
12. Chang, C.-C. (2010). The Duc Kieu, A reversible data hiding scheme using complementary embedding strategy. *Information Sciences, 180*, 3045–3058
13. Zhang, F., Pan, Z., Cao, K., Zheng, F., & Wu, F. (2008). The upper and lower bounds of the information-hiding capacity of digital images. *Information Sciences, 178*(14–15), 2950–2959
14. Chang, C.-C., Lin, C.-Y., & Wang, Y.-Z. (2006). New image steganographic methods using run-length approach. *Information Sciences, 176*, 3393–3408
15. Chang, C.-C., Lin, C.-Y., & Fan, Y.-H. (2008). Lossless data hiding for color images based on block truncation coding. *Pattern Recognition, 41*(7), 2347–2357
16. Sagan, H. (1994). *Space-filling curves*. New York: Springer.
17. Provos, N., & Honeyman, P. (2003). Hide and seek: an introduction to steganography. *IEEE Security & Privacy Magazine, 1*, 32–44
18. Chang, C.-C., Pai, P.-Y., Yeh, C.-M., & Chan, Y.-K. (2010). A high payload frequency-based reversible image hiding method. *Information Sciences, 180*, 2286–2298
19. Chen, P.-Y., & Lin, H.-J. (2006). A DWT based approach for image steganography. *International Journal of Applied Science and Engineering, 4*(3), 275–290
20. Thien, C. C., & Lin, J. C. (2003). A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. *Pattern Recognition, 36*(11), 2875–2881
21. Wang, R. Z., Lin, C. F., & Lin, J. C. (2000). Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition, 34*(3), 671–683
22. Yang, C. H. (2008). Inverted pattern approach to improve image quality of information hiding by LSB substitution. *Pattern Recognition, 41*, 2674–2683
23. Aura, T. (1996). Practical invisibility in digital communication. In: Proceedings of the workshop on information hiding, LNCS 1174 (pp. 265–278).
24. Wang, C. M., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2008). A high-quality steganography method with pixel-value differencing and modulus function. *Journal of System and Software, 81*(1), 150–158
25. Park, Y.-R., Kang, H.-H., Shin, S.-U., & Kwon, K.-R., et al. (2005). An image steganography using pixel characteristics. In Y. Hao (Ed.), *CIS 2005, Part II, LNAI 3802*. (pp. 581–588). Berlin: Springer.
26. Chang, C. C., Chen, T. S., & Chung, L. Z. (2002). A steganographic method based upon JPEG and quantization table modification. *Information Sciences, 141*, 123–138
27. Li, X., & Wang, J. (2007). A steganographic method based upon JPEG and particle swarm optimization algorithm. *Information Sciences, 177*, 3099–3109
28. Raghupathy, B. K., Kumar, N. R., & Raajan, N. R. (2014). An enhanced bishop tour scheme for information hiding. *International Journal of Applied Engineering Research, 9*(1), 145–151
29. Manikandan, G., Bala Krishnan, R., Varadharajan, R., & Dharshini, G. (2014). An 8-queen algorithm based steganographic approach for secure key exchange. *International Journal of Applied Engineering Research, 9*(7), 763–769
30. Ganesh Kumar, K., & Sengan, S. (2020). Improved network traffic by attacking denial of service to protect resource using Z-test based 4-tier geomark traceback (Z4TGT). *Wireless Personal Communications, 114*, 3541–3575. https://doi.org/10.1007/s11277-020-07546-1

31. Yue, Wu., Zhou, Y., Noonan, J. P., & Agaian, S. (2014). Design of image cipher using Latin squares. *Information Sciences, 264*, 317–339
32. Wu, Y., Agaian, S. S., & Noonan, J. P. (2012). Sudoku associated two dimensional bijections for image scrambling. http://arxiv.org/abs/1207.5856.
33. Wu, Y., Zhou, Y., Noonan, J. P., Panetta, K., Agaian, S. (2010). Image encryption using the sudoku matrix. In: S. S. Agaian & S. A. Jassim (Eds.) SPIE, vol. 7708, no. 1, p. 77080P.
34. Hemanth, J., & Uma Maheswari, S. (2017). Performances enhanced image steganography systems using transforms and optimization techniques. *Multimedia Tools and Applications, 76*(1), 415–436
35. Manikandan, G., Krishnan, R. B., Kumar, N. R., Narasimhan, D., Srinivasan, A., & Raajan, N. R. (2018). Steganographic approach to enhancing secure data communication using contours and clustering. *Multimedia Tools and Applications, 77*(24), 32257–32273
36. Manisha, S., & Sree Sharmila, T. (2018). A two-level secure data hiding algorithm for video steganography. *Multidimensional Systems and Signal Processing*. https://doi.org/10.1007/s11045-018-0568-2
37. Ansari, A. S., Mohammadi, M. S., & Parvez, M. T. (2019). A comparative study of recent steganography techniques for multiple image formats. *International Journal of Computer Network and Information Security., 11*(1), 11
38. Manikandan, G., et al. (2019). An approach with steganography and scrambling mechanism for hiding image over images. *International Journal on Emerging Technologies, 10*(1), 64–67
39. Alia, M., & Suwais, K. (2020). Improved steganography scheme based on fractal set. *The International Arab Journal of Information Technology, 17*(1), 128–136

R. Bala Krishnan is working as an Assistant Professor in Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, SASTRA Deemed to be University, kumbakonam from June 2009 onwards. He obtained his M.Tech. at SASTRA and he is now a research scholar at SASTRA, Thanjavur. His areas of interests are Intrusion Detection and Prevention Systems, Information hiding, Image processing and cryptography. He has published over 25 research papers in journals and conferences of repute.

N. Rajesh Kumar received Master degree in Computer Applications from Alagappa University, Karaikudi in 2009. He is an Assistant Professor in the Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, SASTRA Deemed to be University, kumbakonam from June 2010 to now. And he is now a research scholar at SASTRA, Thanjavur. His areas of interests are information hiding, image processing and cryptography. He has published over 15 research papers in journals and conferences of repute.

Dr. N. R. Raajan now working as Senior Assistant Professor in SASTRA Deemed to be University in department of ECE and has teaching experience for about 10 years. He obtained his Ph.D. at SASTRA. He has published more than 200 papers in national and international journals. His area of specialization is Augmented Reality, Hydrophone communication (under water acoustics), Image & Video processing, Signal processing, Wireless communication.

Dr. G. Manikandan is a Faculty Member in the School of Computing, SASTRA Deemed to be University, Tamil Nadu, India. He received his Ph.D. in Computer Science from SASTRA, Tamil Nadu, India. He has published more than 56 technical articles in international journals. His Research interest includes Steganography, Data Mining and Cryptography.

Dr. A. Srinivasan now working as Senior Assistant Professor in SASTRA Deemed to be University in department of ECE and has teaching experience of 16 years. He obtained his Ph.D. at SASTRA. He has published more than 25 papers in national and international journals. He is having Membership in IET, Institution of Engineers (India), Broadcasting Society of India, Having HAM license. Currently he is guiding 4 research scholars.

Dr. D. Narasimhan now working as Associate Professor in SASTRA Deemed to be University in department of Mathematics and has teaching experience for about 22 years. He obtained his Ph.D. at SASTRA. He has published more than 20 papers in national and international journals. His area of specialization is Bitopological spaces. Currently he is working on Graph Theory and Cryptography.

Authors and Affiliations

R. Bala Krishnan[1] · N. Rajesh Kumar[1] · N. R. Raajan[2] · G. Manikandan[3] · A. Srinivasan[4] · D. Narasimhan[5]

R. Bala Krishnan
balakrishnan@src.sastra.edu

N. Rajesh Kumar
rajeshkumar.rb@src.sastra.edu

N. R. Raajan
nrraajan@ece.sastra.edu

A. Srinivasan
srinivasan.a@src.sastra.edu

D. Narasimhan
narasimhan@src.sastra.edu

[1] Department of Computer Science and Engineering, SASTRA Deemed to be University (SRC), Tamil Nadu, India

[2] School of Electrical and Electronics Engineering, SASTRA Deemed to be University, Tamil Nadu, India

[3] School of Computing, SASTRA Deemed to be University, Tamil Nadu, India

[4] Department of ECE, SASTRA Deemed to be University (SRC), Tamil Nadu, India

[5] Department of Mathematics, SASTRA Deemed to be University (SRC), Tamil Nadu, India