*Biomedical Research 2017; 28 (22): 10216-10222* *ISSN 0970-938X*
*www.biomedres.info*

# An adaptive row-column least significant bit inlay approach for image steganography.

**Kommi Sai Siva Satwik, Manikandan C*, Elamaran V, Narasimhan K, Raju N**

School of EEE, SASTRA University, Thanjavur, India

## Abstract

**In a life time, a person visits several hospitals to undergo medical examination for various health issues. When new health issues occur, a record of recent medical reports is necessary for diagnosis. Therefore it is crucial to exchange patient's diagnostic information between the hospitals securely. To transmit such information securely in deceptive environment the effective way is encrypting and hiding it over patient digital photographic image and medical image. Among the various hiding techniques the most widely used technique for medical images is the Least Significant Bit (LSB) substitution technique. Many LSB substitution techniques were developed to enhance both security and image quality of stego-medical images. However, existing approaches were failed to maintain the quality of original images. To overcome this problem we proposed an Adaptive Row-Column (ARC) approach for LSB substitution technique that minimize mean square error (MSE) values and maximize the Peak Signal to Noise Ratio (PSNR) to get both enhanced security and image quality. To further enhance the security and image quality of stego-medical images ARC algorithm is extended to embed both original and inverted cipher text (ARC-OI).**

**Keywords:** Diagnostic information, Data encryption standard, photographic image, Medical image; ARC, ARC-OI.

*Accepted on October 05, 2017*

## Introduction

Steganography is the process of hiding data into images, audio files or video files. Embedding of data into various images like binary images, gray scale images, color images, medical images, texture images, aerial images and so on is called digital image Steganography [1-6]. The data to be hidden in the digital Steganography should be in digital format (0's and 1's). The data may be a text, an image, an audio or a video [1,6]. This data is mainly referred as secret data and the image used to hide this data is named as cover object. The result of embedding the data in the cover object is named as stego object [7-9]. Usually the medical images provide the details of both internal and external organs of the patient [10]. But there is a significant need for transmitting the patient diagnostic information securely over medical images [11,12]. Various hiding techniques like reversible data hiding, multilayer data hiding and EPR hiding have been proposed for medical images [13-15]. These techniques provide security to an appreciable level but failed to improve quality of the stego-medical images. Carrying diagnostic information from one hospital to another hospital without compromising the quality of stego-medical images is a major concern [16]. Two embedding techniques namely spatial domain and frequency domain were used for improving the image quality. Spatial domain directly deals with the pixel arrangement whereas frequency domain deals with the transformed coefficients of cover images [7,17-20]. Many methods have been implemented in the spatial domain technique among which LSB embedding approach is the most commonly used technique. The MSE and PSNR are calculated in order to determine the quality of the image [21]. Security of steganography fails when detected or doubted by a third person [6].Therefore maintaining security and quality of stego images plays a vital role in steganography. Using adaptive random approach (AR) and inverted pattern (IP) approach, both security and quality of the image can be increased significantly [22]. In order to avoid errors in identifying medical image of each patient, integration of photographic and medical image was done. These integrations act as identification tools [23,24]. Medical images obtained from CR, MR and CT scans are stored in digital format that contain details of the patient and information about the study [25]. In this paper, an Adaptive Row-Column (ARC) embedding algorithm is implemented for carrying diagnostic information over medical and photographic images with high security and quality. Also ARC is extended to embed original and inverted information (ARC-OI) to further increase security and quality of stego images significantly.

## Materials and Methods

### *System model*

At the sender side patient's photographic image and medical image are captured using a single digital camera with mode select option as shown in Figure 1. The images getting from

camera are considered as cover images. Simultaneously respective patient's diagnostic information is encrypted using DES algorithm. The encrypted diagnostic information is fed as input for embedding process. The proposed ARC algorithm is applied resulting in stego image and a dynamically generated key. This stego image and secret key is communicated from one hospital to another or from one doctor to the other through secure means of communication.

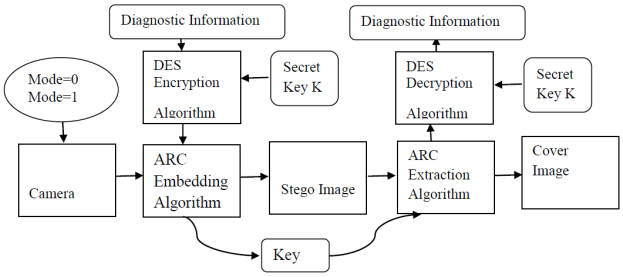


***Figure 1.*** *Framework of the proposed system.*

On other side stego image and secret key are fed into ARC extraction algorithm to extract encrypted diagnostic information. This information is fed into DES algorithm to obtain decrypted diagnostic information.

In ARC algorithm, for embedding each cover image is divided into equal blocks of 8×8 pixels. Then each block is selected randomly only once for embedding the cipher text by following all the random paths namely Straight Up (SU), Straight Down (SD), Flipped Up (FU), Flipped Down (FD), Straight Forward (SF), Straight Backward (SB), Flipped Forward (FF) and Flipped Backward (FB).

In Figure 2 straight down approach embedding is done column wise from top to bottom throughout the selected block in the ascending order of numbers.

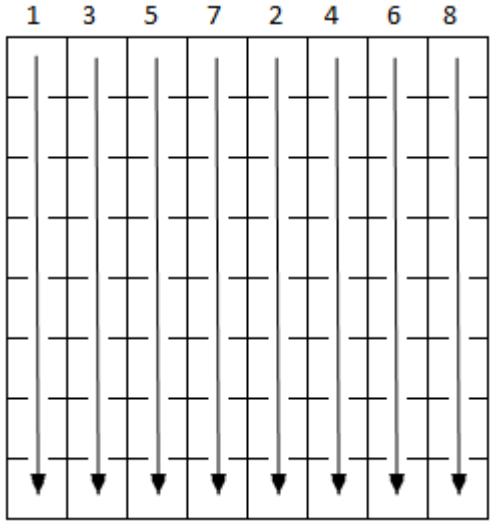


***Figure 2.*** *Straight Down (SD) approach of embedding.*

In Figure 3 straight up embedding is done column wise from bottom to top throughout the selected block in the ascending order of numbers.

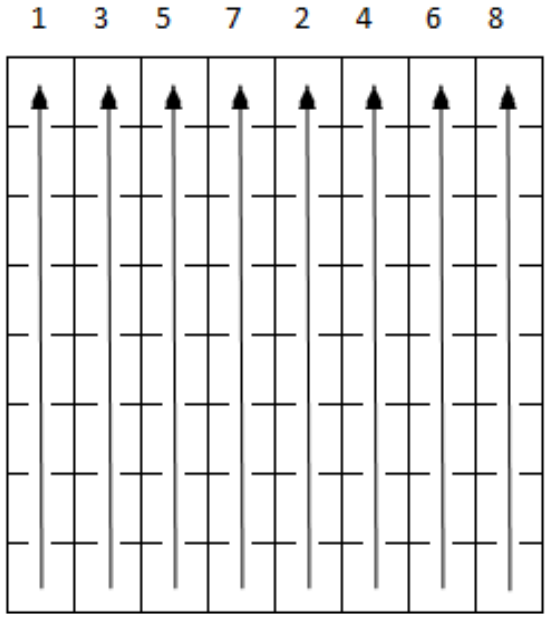


***Figure 3.*** *Straight Up (SU) approach of embedding.*

In Figure 4 straight forward approach embedding is done row wise from left to right throughout the selected block in the ascending order of numbers.

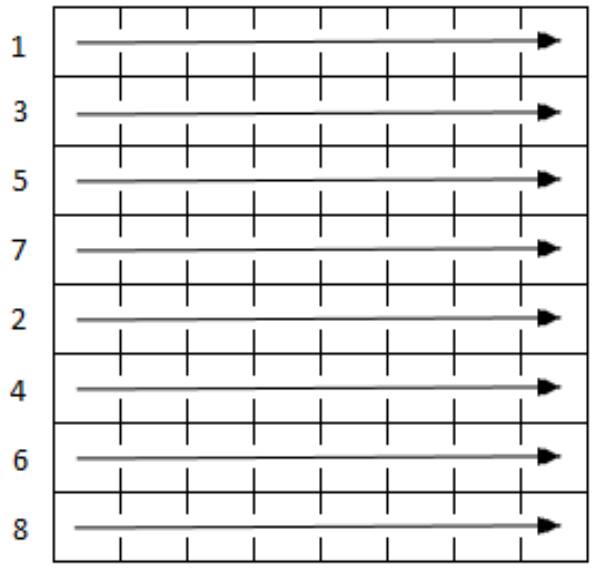


***Figure 4.*** *Straight Forward (SF) approach of embedding.*

In Figure 5 straight backward embedding is done row wise from right to left throughout the selected block in the ascending order of numbers.

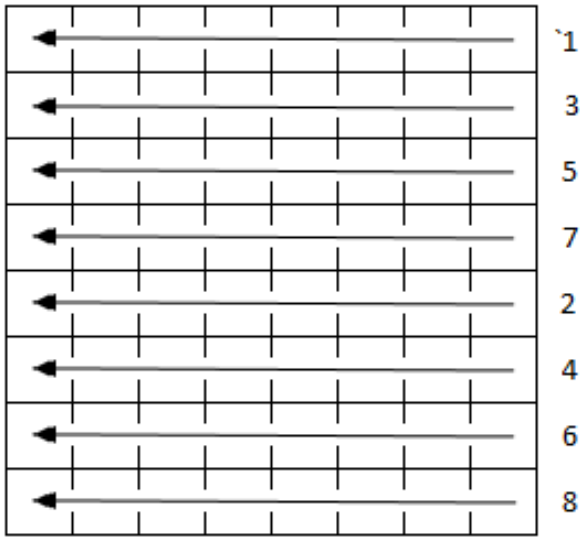


*Figure 5. Straight Backward (SB) approach of embedding.*

In Figure 6 flipped up approach embedding is done column wise in the ascending order of numbers. First half of the selected blocks are embedded from bottom to top and remaining blocks are embedded from top to bottom.

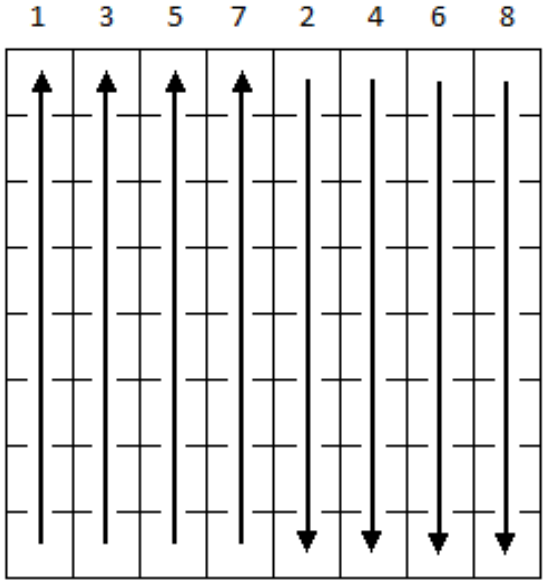


*Figure 6. Flipped Up (FU) approach of embedding.*

In Figure 7 flipped down approach embedding is done column wise in the ascending order of numbers. First half of the selected blocks are embedded from top to bottom and remaining blocks are embedded from bottom to top.

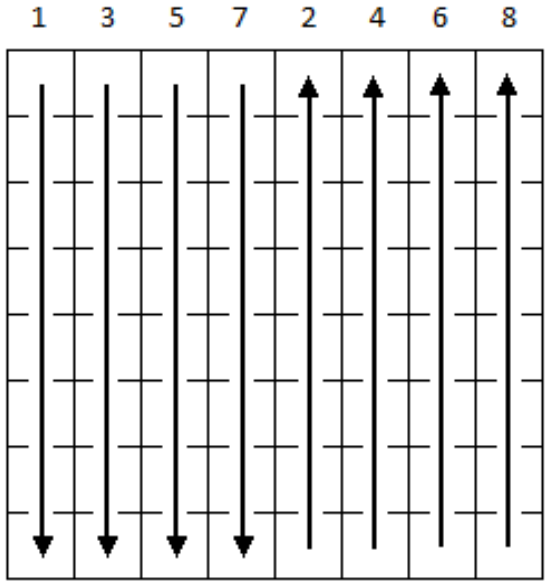


*Figure 7. Flipped Down (FD) approach of embedding.*

In Figure 8 flipped forward approach embedding is done row wise in the ascending order of numbers. First half of the selected blocks are embedded from left to right and remaining blocks are embedded from right to left.

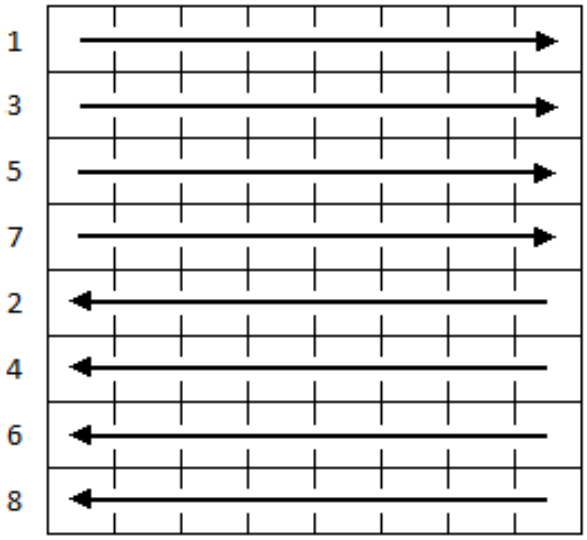


*Figure 8. Flipped Forward (FF) approach of embedding.*

In Figure 9 flipped backward approach embedding is done row wise in the ascending order of numbers. First half of the selected blocks are embedded from right to left and remaining blocks are embedded from left to right.

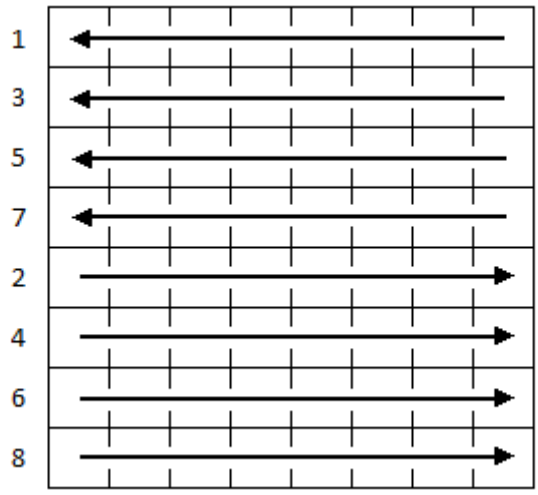


*Figure 9. Flipped Backward (FB) approach of embedding.*

## Algorithm for Embedding

**Inputs:** Cover image C, cipher text T

**Outputs:** Stego image S, key K

1. Generate cipher text bit stream 'B' from the plain text 'P' by applying DES algorithm.

2. Divide the cover image C into 8×8 pixels of blocks or 4×4 pixels of blocks.

3. Consider a random function that generates random numbers without repetition. This random number is implicated to each block. Therefore, the range of random function is 0 to total number of blocks.

4. Select a random block by using random function and embed original cipher text bit stream B using all random paths mentioned above for that block.

5. Invert the cipher text bit stream B to obtain inverted cipher text bit stream I.

6. Apply all random paths for inverted cipher text bit stream I.

7. Calculate MSE for all the patterns with original and inverted cipher text bit stream and fix the pattern with least MSE for that block.

8. If the pattern with least MSE is for inverted cipher text I, then, set the least significant bit of the key K as '1'. Otherwise, set it as '0'.

9. Shift the secret key K to the left by 3 bits. Modify the 3 least significant bits of the key based on the pattern selected referring to Table 1. Shift the secret key K to the left by 1 bit.

10. Repeat from step 4 until every block is filled with encrypted data.

11. Generate stego image and secret key

12. Transmit stego image and the secret key.

**Generating key:** Key is dynamically generated based on Table 1. Let K be the key and three bits at a time are modified based on the selection of the pattern for that block. This selection is repeated for all the blocks.

*Table 1. Key bits based on the pattern selected for embedding.*

| Pattern | K [3i+2] | K [3i+1] | K [3i] |
|---|---|---|---|
| Straight Up (SU) | 0 | 0 | 0 |
| Straight Down (SD) | 0 | 0 | 1 |
| Straight Forward (SF) | 0 | 1 | 0 |
| Straight Backward (SB) | 0 | 1 | 1 |
| Flipped Up (FU) | 1 | 0 | 0 |
| Flipped Down (FD) | 1 | 0 | 1 |
| Flipped Forward (FF) | 1 | 1 | 0 |
| Flipped Backward (FB) | 1 | 1 | 1 |

Therefore, the length of the key generated by using this random path approach is calculated as follows;

For block of 8×8 pixels, key length = 1024 × 4=4096 bits.

For block of 4×4 pixels, key length = 4096 × 4=16384 bits.

## Algorithm for Extracting

**Inputs:** Stego object S, Key K

**Outputs:** Cipher Text C

1. Read the Stego object S

2. Read the Key K

3. Use the same random function that is used while embedding to select the respective block.

4. Extract only 4 least significant bits from total length of the key size K. let the extracted bit stream be E.

5. Based on 3 least significant bits of E, retrace the determined random path in that block by referring to Table 1 to retrieve the encrypted data bits from that block.

6. If the most significant bit of E is '1' then, invert the obtained encrypted data bits to get original encrypted data bits. Otherwise, continue to step 7

7. Repeat from step 4 until all the encrypted data bits are extracted.

8. Obtain the bit stream B of the encrypted data from the extracted bits.

9. Decrypt the data using DES algorithm with the help of the key that was used while generating cipher text T.

10. Write the data obtained into an output file.

## Error and Peak Signal to Noise Ratio Calculation

Error calculation places a crucial role in embedding the secret data in an image. The lower value of MSE provides the higher values of PSNR which means higher the image quality.

Mean Square Error (MSE) of each block is calculated by the formula:

$$MSE = \frac{1}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(Cij - Sij)^2\right)$$

Where, M and N are width and length of the block respectively. $C_{ij}$ is the value of cover image pixel and $S_{ij}$ is the value of stego image pixel.

Similarly, Peak Signal to Noise Ratio can be measured using the formula:

$$\text{PSNR (dB)} = 10\log_{10}\left(\frac{i_{\max}^2}{MSE}\right)$$

Where, $I_{max}$ is the maximum intensity of a pixel. For a grayscale image $I_{max}$=255.

## Results and Discussion

The proposed ARC algorithm is adopted for 4 different grayscale photographic and medical images as shown in Figure 10 and Figure 11. Then, MSE values and PSNR values for ARC algorithm is compared with the existing methods Z scan SFC (Space Filling Curve), Hilbert scan SFC, ZigZag scan SFC, Moore scan SFC [22] and Adaptive Random technique (AR) and the results are provided in Table 2. It is observed from the results that MSE value is minimized and PSNR value is maximized for ARC algorithm.

*Figure10. Cover images a) Lena b) Rob c) John d) Jennifer.*

*Figure11. Medical Images a) Lena b) Rob c) John d) Jennifer.*

This provides evidence to conclude that quality of the stego image is increased using ARC algorithm. Further the proposed ARC algorithm is extended to embed both original and inverted cipher text (ARC-OI) and its results are compared with ARC algorithm for the same cover image. The results provided in Table 3 shows that the quality of stego image is further increased.

*Table 2. Comparison of ARC with Z scan SFC, Hilbert scan SFC, ZigZag scan SFC ,Moore scan SFC and AR algorithm.*

| | Pattern | K=1 | | | | K=2 | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | MSE 4X4 | PSNR 4X4 | MSE 8X8 | PSNR 8X8 | MSE 4X4 | PSNR 4X4 | MSE 8X8 | PSNR 8X8 |
| Cover Image | ZS | 0.5001 | 51.1221 | 0.4985 | 51.1541 | 2.5846 | 44.0068 | 2.5752 | 44.0225 |
| | HS | 0.5000 | 51.1010 | 0.4985 | 51.1583 | 2.5761 | 44.0210 | 2.5695 | 44.0321 |
| | ZigS | 0.5000 | 51.1414 | 0.4991 | 51.1488 | 2.5905 | 43.9969 | 2.5732 | 44.0259 |
| | MS | 0.5016 | 51.1371 | 0.4994 | 51.1458 | 2.5829 | 44.0097 | 2.5906 | 43.9967 |
| | AR | 0.4217 | 51.8799 | 0.4519 | 51.5794 | 2.1903 | 44.7256 | 2.3611 | 44.3996 |
| | ARC | 0.3699 | 52.4499 | 0.4271 | 51.8255 | 2.0925 | 44.9241 | 2.2741 | 44.5627 |
| Lena's MI | ARC | 0.3818 | 52.3124 | 0.4241 | 51.8561 | 2.0324 | 45.0507 | 2.1076 | 44.8929 |

*Table 3. Comparison of ARC approach and ARC-OI.*

| Cover Image | Pattern | K=1 | | | | K=2 | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | MSE 4X4 | PSNR 4X4 | MSE 8X8 | PSNR 8X8 | MSE 4X4 | PSNR 4X4 | MSE 8X8 | PSNR 8X8 |
| Lena | ARC | 0.3699 | 52.4499 | 0.4271 | 51.8255 | 2.0925 | 44.9241 | 2.2741 | 44.5627 |
| | ARC-OI | 0.3068 | 53.2622 | 0.3960 | 52.1538 | 2.0454 | 45.0537 | 2.0916 | 44.9260 |
| Lena's MI | ARC | 0.3818 | 52.3124 | 0.4241 | 51.8561 | 2.0324 | 45.0507 | 2.1076 | 44.8929 |
| | ARC-OI | 0.3226 | 53.0441 | 0.3993 | 52.1178 | 1.9315 | 45.2718 | 2.0326 | 45.0502 |
| Rob | ARC | 0.4067 | 52.0380 | 0.4462 | 51.6355 | 2.0847 | 44.9403 | 2.2413 | 44.6258 |
| | ARC-OI | 0.3317 | 52.9233 | 0.4031 | 52.0766 | 2.0153 | 45.0874 | 2.1082 | 44.8916 |
| Rob's MI | ARC | 0.3709 | 52.4382 | 0.4262 | 51.8346 | 2.1845 | 44.7372 | 2.2742 | 44.5625 |
| | ARC-OI | 0.3103 | 53.2129 | 0.3967 | 52.1461 | 2.0863 | 44.9370 | 2.1941 | 44.7182 |
| John | ARC | 0.3787 | 52.3478 | 0.4291 | 51.8052 | 2.0962 | 44.9164 | 2.1484 | 44.8096 |
| | ARC-OI | 0.3132 | 53.1725 | 0.3957 | 52.1571 | 1.9794 | 45.1654 | 2.0884 | 44.9326 |
| John's MI | ARC | 0.3737 | 52.4055 | 0.4276 | 51.8204 | 2.1304 | 44.8461 | 2.2051 | 44.6965 |
| | ARC-OI | 0.3142 | 53.1587 | 0.4008 | 52.1015 | 2.0142 | 45.0897 | 2.1197 | 44.8680 |
| Jennifer | ARC | 0.3788 | 52.3467 | 0.4243 | 51.8540 | 2.0911 | 44.9270 | 2.1562 | 44.7939 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | ARC-OI | 0.3184 | 53.1010 | 0.3969 | 52.1439 | 2.0021 | 45.1159 | 2.0844 | 44.9409 |
| Jennifer's MI | ARC | 0.3838 | 52.2897 | 0.4295 | 51.8011 | 2.0681 | 44.9750 | 2.1562 | 44.7939 |
| | ARC-OI | 0.3180 | 53.1065 | 0.3988 | 52.1232 | 2.0362 | 45.0425 | 2.1546 | 44.7971 |

## Complexity Level Estimation

To estimate complexity level of the proposed algorithm the entire 256×256 cover image divide into 8×8 blocks which yields 1024 blocks. Total number of ways in which 1024 blocks can be selected is (1024)! The filling of data in each block is done in 8 ways based on each pattern mentioned above. According to DES data in each block can be deciphered through brute force attack by 264 ways. Therefore, Total complexity expected is 264 × 8 × (1024)! This complexity level is further increased by changing the starting position of data in each block which can be done in 64 ways. Therefore, total complexity expected is 264 × 8 × (1024)! × 64. Even more complexity can be achieved by embedding both original and inverted cipher text into each block and selecting the pattern with least MSE. This can be done in 2 ways. Hence, for a 256×256 image divided into 8×8 blocks and with inverted pattern of data total complexity level estimation is 264 ×8 × (1024)! × 64 × 2.

Similarly by dividing 256×256 cover image into 4×4 blocks the estimated complexity level is 264 ×8 × (4096)! × 64 × 2.

## Conclusion

In this paper an ARC and ARC-OI embedding algorithms were implemented to embedded patient's diagnostic information over their photographic and medical images. The proposed approach provided an improved image quality and security compared to existing approach. In addition, it is also observed that the generated key for each cover image is unique. This shows the robustness of this approach and increased security against brute force attacks hence, using this proposed technique, medical reports of the patients at different hospitals can be transmitted securely with enhanced medical image quality.

## References


1. Bender W, Butera W, Gruhl D, Hwang R, Paiz F J, Pogreb S. Applications for data hiding, IBM Sys J 2000; 39: 547-568.
2. Bender W, Gruhl D, Morimoto N, Lu A. Techniques for data hiding, IBM Sys J 1996; 35: 313-336.
3. Chan CK, Chen LM. Hiding data in images by simple LSB substitution. Pattern Recog 2004; 37:469-474.
4. Katzenbeisser S, Petitcolas FAP. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House 2000.
5. Ni Z, Shi YQ, Ansari N, Su W. Reversible Data Hiding. IEEE transactions on circuits and systems for video technology 2006; 354-362.
6. Petitcolas FAP, Anderson RJ, Kuhn MG. Information hiding – a survey. Proc IEEE 1999; 87:1062-1078.
7. Aura T. Practical invisibility in digital communication. International Workshop on Information Hiding 1996: 265-278.
8. Chang CC, Kieu TD. A Reversible Data Hiding Scheme Using Complementary Embedding Strategy. Inform Sci 2010; 180: 3045-3058.
9. Provos N, Honeyman P. Hide and seek: an introduction to steganography. IEEE Security & Privacy Magazine 2003; 1: 32-44.
10. Mclnerny T, Terzopoulos D. Deformable models in medical image analysis. Medical Image Analysis, Workshop on Mathematical Methods in Biomedical Image Analysis 1996: 171-180.
11. Rudi Van de Velde, Patrice Degoulet. Clinical Information Systems A Component Based Approach. Springer-Verlag New York, Inc. 2003.
12. Sergio SF, Marina SR, Ramon, AM, Marcelo S, Nivaldo B, Gustavo HMBM. Managing medical images and clinical information. IEEE Trans Inf Technol Biomed 2007; 11: 17-24.
13. Dasa A, Islama S, Guptab S, Guptaa P. Data Hiding in Medical Images. Journal of computers 2014; 9: 513-518.
14. Lou DC, Hu MC, Liu JL. Multiple layer data hiding scheme for medical images.Computer Standards & Interfaces 2009; 31: 329-335.
15. Navas KA, Archana Thampy S, Sasikumar M. EPR Hiding in Medical Images for Telemedicine. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering 2008; 2: 223-226.
16. Singh H, Naik AD, Rao R, Petersen LA. Reducing Diagnostic Errors through Effective Communication: Harnessing the Power of Information Technology. J Gen Intern Med 2008; 23: 489-494.
17. Chang CC, Lin CY, Wang YZ. New image steganographic methods using run-length approach. Inform Sci 2006; 176: 3393-3408.
18. Chang CC, Pai PY, Yeh CM, Chan YK. A high payload frequency-based reversible image hiding method. Inform Sci 2010; 180: 2286-2298.
19. Thien CC, Lin JC. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recognition 2003; 36: 2875-2881.
20. Wang RZ, Lin CF, Lin JC. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition 2000; 34: 671-683.
21. Tan HL, Li Z, Tan YH, Rahardja S, Yeo C. A Perpetually Relevant MSE Based Image Quality Metric. IEEE Transactions on Image Processing 2013; 22: 4447-4459.

22. Amirtharajan R, Rayappan JBB. An Intelligent Chaotic Embedding Approach to Enhance Stego-Image Quality. Information Sciences 2012; 193: 115-124.
23. Ramamurthy S, Bhatti P, Arepalli CD, Salama M, Provenzale JM, Tridandapani S. Integrating patient digital photographs with medical imaging examinations. J Digit Imaging 2013; 26: 875-885.
24. Tridandapani S, Berkowitz E, Bhatti P. Integrating digital photographs with medical image examinations. IEEE EMBS Conference on Biomedical Engineering & Sciences 2010: 184-187.
25. Rodriguez-Colin R, Feregrino-Uribe C, Trinidad-Blas G. Data Hiding Schemes for Medical Images. 17th International Conference on Electronics, Communications and Computers 2007; 1-6.

***Correspondence to**

C. Manikandan

Department of ECE

School of EEE

SASTRA University

India