A Reversible Data Hiding through Encryption Scheme for Medical Image Transmission Using AES Encryption with Key Scrambling

Kandala Sree Rama Murthy and V. M. Manikandan
Computer Science and Engineering, SRM University-AP, Andhra Pradesh, India
Email: {kandala_sree, manikandan.v}@srmap.edu.in

***Abstract*—Reversible Data Hiding (RDH) is an active area of research having numerous applications in the field of medical image transmission for transmitting clinical reports along with medical images. The existing RDH schemes are categorized into RDH in natural images, RDH in encrypted images, and RDH through encryption. In this research work, we have considered RDH through encryption and used advanced standard encryption techniques. An RDH through encryption scheme in medical image transmission will take a medical image, a clinical report (text file) and an encryption key as inputs and produce an encrypted image as the output. Note that the clinical report is embedded in the medical image as part of the encryption process. In the proposed scheme, the original image is divided into non-overlapping blocks, and AES encryption is performed on each block to get the encrypted image. The key used in AES encryption is scrambled by Arnold transform d times for each block, where d is the data bit that is to be embedded in that block. At the receiver side, the data extraction and image restoration will be carried by analyzing the texture property of image blocks generated through the AES decryption process with all the Arnold transform versions of the AES key. The experimental study is done on medical and natural images to analyze various efficiency parameters such as embedding rate, bit error rate, Peak Signal to Noise Ratio (PSNR), and Structural Similarity Index (SSIM).**

***Index Terms*—reversible data hiding, medical image transmission, AES encryption, Arnold transform**

I. Introduction

Data hiding methods and image encryption techniques have been widely used for information security in the last three decades [1], [2]. The data hiding helps to transmit the secret data by hiding it using a cover medium. The encryption methods help to convert the data into an unreadable form to ensure that only the authorized person will be able to read the contents after decryption. Reversible Data Hiding (RDH) is an area where extensive research has been done in recent days. The basic feature of an RDH scheme is that the cover medium used for data hiding can be restored by the authorized after the extraction of the hidden message [3]-[6].

Manuscript received August 26, 2021; revised December 29, 2021; accepted January 26, 2022.

Digital images are widely used as the cover medium, and in this research work also we have considered digital images. The RDH schemes in images are mainly categorized into three based on the way and kind of data hiding process:

- RDH in natural images: The data hiding process will be performed on the original image [7]-[10].
- RDH in the encrypted image: The data hiding will be performed on the encrypted image. The data hider cannot see any content of the actual image since it is in the encrypted form [11]-[14].
- RDH through encryption: This scheme combines both the image encryption process and the data hiding into a single process. The scheme will take an image and the message, and the output will be an encrypted image [15]-[19].

The first RDH through encryption scheme was introduced in 2019 [15]. This research work focuses on RDH through encryption. In this manuscript, we have introduced an RDH through encryption scheme which uses Advanced Encryption Standards (AES) [20] for image encryption with a well-known image scrambling scheme called Arnold transform [21], [22].

The novelty of the proposed scheme is listed below:

- RDH in natural images: The data hiding process will be performed on the original image [7]-[10].
- All the existing RDH through encryption schemes used stream cipher encryption methods, but in the proposed scheme, for the first time, we introduced the use of AES image encryption for achieving the benefits of image encryption and reversible data hiding.
- The Arnold transform is used for scrambling the AES key after creating a 2D array based on a predefined function.
- We have achieved a very good embedding rate compared to the other RDH through encryption schemes.

The contents of this manuscript are arranged as follows: Section II gives a brief overview of the existing RDH through encryption and compares their properties. Section III explains the proposed schemes with detailed pseudo-code and illustrative diagrams. Section IV has a detailed experimental study that we have done and the observation results. The comparative study is also done in Section IV.

doi: 10.12720/jait.13.5.433-440

Section V concludes the manuscript with the scope of future works in this domain.

II. Related Work

As discussed in the introduction, we have proposed a new RDH through encryption that uses AES encryption with Arnold transform. So in this section, we reviewed the RDH through encryption schemes.

The first RDH through encryption scheme was introduced in 2019 [15]. In this scheme, the sender and receiver used three different encryption keys: K_1, K_2, and K_3, and the non-overlapping blocks encrypted using the stream ciphers generated by the encryption key. The authors used the RC4 stream generator in this work. The selection of a stream cipher for encrypting a block is decided by the data bit that the data hider wants to hide in the selected block. The scheme allows hiding one bit in a block of size B×B pixels. The experimental results showed that most of the images recover correctly while using a block size of 8×8 pixels. A Support Vector Machine (SVM) model is trained during the experimental study of the scheme. The SVM model is trained in such a way that it can classify a given image block into a natural image block or encrypted image block based on the randomness of the pixels in the image block.

Since the scheme reported in [15] has the overhead of training the SVM model, in 2019, a scheme that uses a statistical measure based on entropy for image recovery is discussed in [16]. The entropy-based RDH through the encryption scheme reported a better bit error rate than the previous scheme.

A scheme to improve the embedding rate by generating the number of stream ciphers by performing predefined operations on the stream ciphers generated using three keys is discussed in [17]. This scheme ensured a higher embedding rate as compared to previous schemes. But the image encryption time and image restoration time were a bit higher. Another scheme is discussed in [18], which uses block pre-checking to ensure 100% image recovery at the receiver-side.

In 2021, a rotated stream cipher approach that uses only one encryption key K is introduced in [19]. The scheme ensured a good embedding rate since only one encryption key was used in this scheme which reduces the overhead of key handling. The existing RDH through encryption schemes is compared in Table I.

TABLE I. Comparison of Existing RDH through Encryption Schemes

Method	Encryption Scheme used	Approach for image recovery	Number of keys used
Scheme in [15]	RC4	Trained SVM model is used	3
Scheme in [16]	RC4	Entropy measure is used	3
Scheme in [17]	RC4	Trained SVM model is used	3
Scheme in [18]	RC4	Trained SVM model is used	3
Scheme in [19]	RC4	A smoothness measure by comparing adjacent pixels	1

From the detailed literature review, we have identified the following challenges in this domain:

- All the existing RDH through encryption scheme uses stream cipher based image encryption process which is having many security falls.
- The overhead in handling encryption and/or decryption is high due to the number of keys used in the process.
- Most of the existing schemes use trained machine learning models for image recovery and data extraction. The overhead of training is one concern, and the trained model should be handed over to the receiver for image recovery purposes.
- Most of the RDH through encryption schemes provide a high embedding rate as compared to the RDH schemes in encrypted images. But still, the embedding rates are not good enough to use in practical applications.

In this research work, our objective is to design and implement an RDH through an encryption scheme for secure medical image transmission with a high embedding rate without compromising image recoverability and data extraction. The encryption process also should be secure enough with minimum overhead in key sharing. By considering these objectives, we introduced a new RDH through an encryption scheme, which uses one of the well-known image encryption schemes called AES with Arnold key scrambling.

III. Proposed Scheme

The proposed reversible data hiding through an encryption scheme for embedding clinical reports in the medical image is discussed in this section. The proposed software system can be classified into two modules:

1) Sender-side module: The sender-side module will take a medical image, the clinical report of the patient, and the AES encryption key as the inputs, and it will generate an encrypted image as the output, which will be embedded with the clinical report. The overview of the sender-side module is shown in Fig. 1.
2) Receiver-side module: The receiver will get one medical image which will be in encrypted form. The sender is expected to share the AES encryption key details prior. The receiver-side module will be capable of decrypting the medical image to get back the original medical image used by the sender, and also the receiver-side module will output the clinical report. The overview of the sender-side module is shown in Fig. 2.

The proposed RDH through the encryption scheme is described in Algorithm 1. The image restoration and clinical report extraction scheme are in Algorithm 2. Fig. 3 shows the flow diagram of proposed scheme.

The process of finding the smoothness measure of an image block H having size B×B pixels is given in (1).

$$S = \sum_{x=1}^{B} \sum_{y=1}^{B-1} |H_{x,y} - H_{x,y+1}| \quad (1)$$

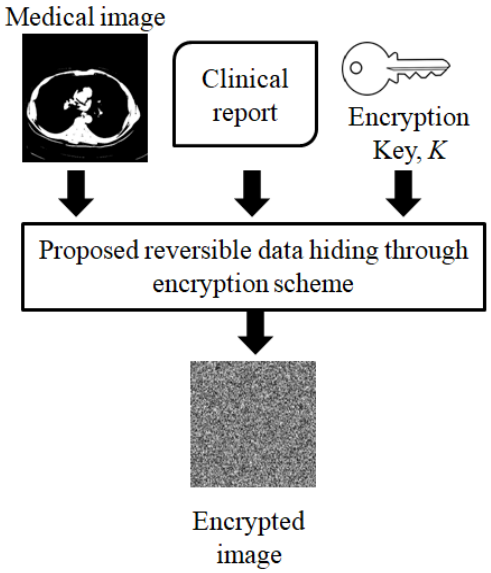

Figure 1. Overview of the sender-side module of the proposed scheme.

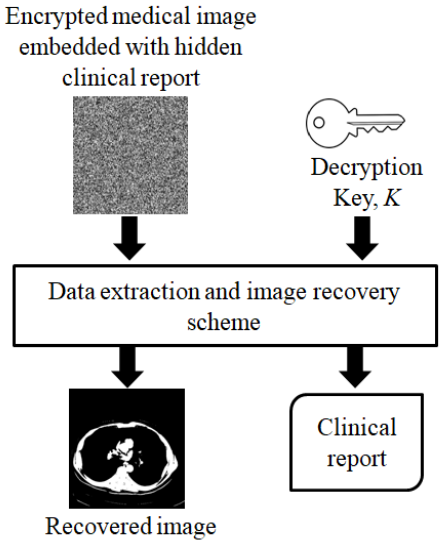

Figure 2. Overview of the receiver-side module of the proposed scheme.

ALGORITHM 1: Proposed RDH through encryption scheme to hide clinical report in the medical image using AES and Arnold transform

INPUT: The medical image *M*, the clinical report *L*, AES encryption key *K*

OUTPUT: The encrypted medical image *E* with the hidden clinical report

1 Initialize a 2D array *E* with zeros of the same size as the given medical image *M*. This 2D array will be used to store the final encrypted image.
2 Divide the medical image *M* into partitions in such a way that each partition will have a size of $B \times B$ pixels.
/* We have considered B = 8 */
3 Find the periodicity *P* of Arnold transform when the image block has a size $B \times B$ pixels.
4 Generate a 2D array *K*' of size $B \times B$ by tiling the 4×4 AES key. Without loss of generality, assume that $B = 4 \times Q$, where *Q* is an integer.
5 Convert the characters in clinical report *L* to the corresponding sequence of bits *T*. Each character in the report can be converted into its corresponding 8 bits.
6 Convert the sequence of bits *T* into the sequence of numbers with base *P*. Let us denote the resultant sequence numbers by *D*. Note that each of the elements from the sequence *D* can be embedded into an image block of size $B \times B$ pixels.
7 Let us denote the blocks in the M^k where k= ⌊R/B⌋ ⌊C/B⌋. Let us assume that we are processing the blocks from the image in row-wise linear order. Let us assume that the data sequence *D* also will have *k* number of values.
8 Consider k^{th} value, say D^K from *D*. Then apply D^K number of Arnold transforms on *K'* to *K''*.
9 Access the k^{th} block from the image *M*, say M^k. Divide M^k into sub-blocks of size 4×4 and encrypt each sub-block using AES encryption algorithm by passing corresponding sub-block of *K''* as the key. Let us say the resultant encrypted image block is W^k
10 Keep W^k as *the* k^{th} block in 2D array *E*.
11 Increment the *k* value by 1.
12 Repeat step 8 to step 10 until the block of the medical image *M* is encrypted.
13 Repeat the final medical encrypted image *W* with a hidden medical report.

ALGORITHM 2: Proposed RDH through encryption scheme to hide clinical report in the medical image using AES and Arnold transform

INPUT: The encrypted medical image W, AES decryption key K

OUTPUT: The restored medical image M, the extracted clinical report L

1 Initialize a 2D array *M* with zeroes of the same size as given encrypted medical image *W*. This 2D array will be used to store the final recovered medical image
2 Divide the medical image *W* into partitions in such a way that each partition will have a size $B \times B$ pixels.
/* We have considered B=8*/
3 Find the periodicity *P* of Arnold transform when the image block has size $B \times B$ pixels.
4 Generate a 2D array *K'* of size $B \times B$ by tiling the 4×4 AES key without loss of generality assume that $B = 4 \times Q$, where Q is a positive integer.
5 Initialize an empty list *T* to store the extracted information. Each time while performing the data extraction, we will get a value *Z* from each block where Zϵ{0,1,2,…, P-1}. Note that *P* is the periodicity of Arnold transform when the block size is $B \times B$.
6 Let us denote the blocks in the W^G where G= ⌊R/B⌋ ⌊C/B⌋. Let us assume that we are processing the blocks from the image in row-wise linear order (the same order we follow while data hiding).
7 Apply *P* number of Arnold transforms on *K'* to generate *P* different versions of AES key. Let us denote the versions of AES keys getting after Arnold transform by (K'^0, K'^1, K'^2,…,$K'^{(P-1)}$).
8 Access G^{th} block from the image *W*, say W^G, and decrypt the same block using AES decryption scheme by passing *K'Y* as the key, where $Y = 0, 1, 2, \ldots, P - 1$. Let us say the resultant decrypted versions of the image block are H^Y.
9 Analyze the naturalness of the image blocks using the smoothness measure. The smoothness measure is computed by using equation (1). Find the smoothness O^Y measure from all the image blocks H^Y.
10 Find the minimum value from the sequence $(O^0, O^1, \ldots, O^{P-1})$. Let us assume O^v is the minimum value.
11 The extracted data from the G^{th} block will be *V*, and the recovered medical image block will be H^v.
12 Append *V* at the end of *T*.
13 Replace the block M^G with H^v.
14 Repeat the process from step 6 to step 12 to get back the recovered medical image.
15 Convert *T* to its corresponding binary sequence and further convert the same to 8-bit characters to get the final text document. Say, the final report is *L*.
16 Return recovered medical image *M* and the extracted clinical report *L*.

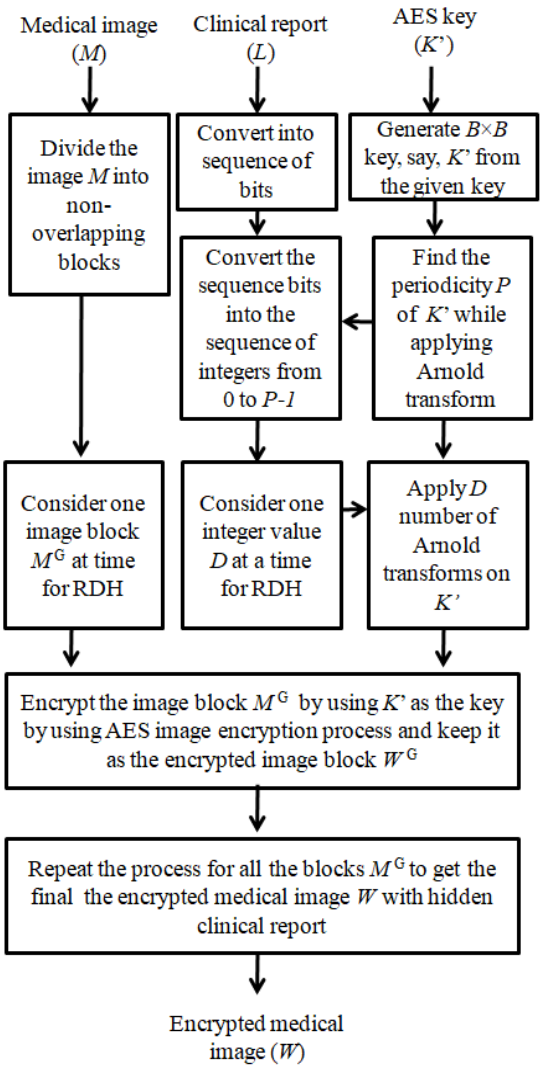

Figure 3. Flow diagram of the proposed scheme.

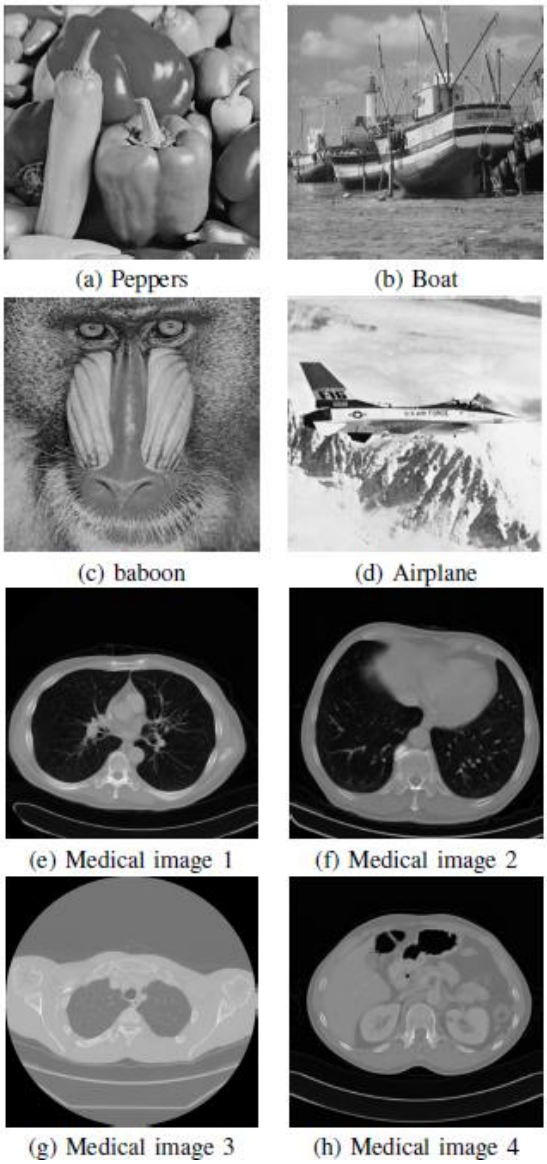

Figure 4. Sample images considered during the experimental study.

IV. Experimental Study and Result Analysis

This section discusses the experimental study and results analysis. We have conducted an experimental study on both natural images and medical images [23], [24]. The implementation of the proposed scheme is done using MATLAB 2021.

The experimental study is done on a large-scale natural image dataset and medical image from a standard image dataset. For results, we have considered 4 well-known natural images and 4 medical images to show the results in a compact way. Note that the selected 4 natural images have completely different characteristics, and if a scheme works for these images, there is a very high probability that the scheme will work for most of the other images until unless no exceptional features in the images. The 8 images that we have considered during the experimental study are given in Fig. 4.

The following efficiency measures are analyzed to check the efficiency of the newly introduced scheme:

A. Analysis of Embedding Rate and Bit Error Rate

Embedding Rate *(ER)*: This measure decides the amount of data that we can hide in the medical image during the data hiding process. Readers may note that the embedding rate of the RDH scheme is not unlimited. Mathematically ER is defined as follows:

$$ER = \frac{\text{Number of bits that can be embedded}}{\text{Total number of pixels in the image}} \quad (2)$$

A good RDH through an encryption scheme should provide a high embedding rate to ensure the embedding of lengthy messages. The embedding rate obtained from all the selected 8 images are given in Table II.

TABLE II. EMBEDDING RATE OF THE PROPOSED SCHEME FOR SELECTED WELL-KNOWN IMAGES

Image name	Embedding rate (bits per pixels)
Natural Images	
Baboon	0.0539
Airplane	0.0539
Peppers	0.0539
Boat	0.0539
Medical Images	
Medical image 1	0.0539
Medical image 2	0.0539
Medical image 3	0.0539
Medical image 4	0.0539

The proposed scheme's embedding rate will depend on the block size that we use during data hiding.

If we use a block size $B \times B$ pixels and the Arnold transform periodicity of a 2D array of size $B \times B$ is P, then the embedding rate $ER^{Proposed}$ from the proposed scheme will be

$$ER^{Proposed} = \frac{Log_2(P-1)}{B \times B} \quad \text{bpp} \tag{3}$$

The relationship between the Arnold transform periodicity, and the embedding rate is shown in Table III.

TABLE III. RELATIONSHIP BETWEEN EMBEDDING RATE AND BLOCK SIZE

S. No.	Block Size	Base of number system	Range of decimal numbers embedded within a block	ER (bpp)
1	4×4	6	0-5	0.1450
2	8×8	12	0-11	0.0539
3	16×16	24	0-23	0.0176
4	32×32	48	0-47	0.0054

From Table III, it can be observed that a larger block size will reduce the embedding rate. So we prefer to use a small block size in the proposed algorithm to ensure a high embedding rate. But the use of small block sizes such as 4×4 pixels leads to an error during image recovery.

From the experimental study, it is observed that the proposed scheme has successfully recovered all the images while using a block size of 8×8 pixels, which yields an embedding rate of 0.0539 bpp.

Bit Error Rate (BER): This parameter gives an idea about the quality of message extraction. The BER is defined as follows:

$$BER = \frac{\text{Number of bits wrongly extracted}}{\text{Total number of bits in the message}} \tag{4}$$

The proposed scheme has the property that if the image is recovered correctly, then the extraction of hidden messages is also successful. We have observed a BER of 0 from all the experimental images.

B. Analysis of Randomness in the Encrypted Images

The randomness in the encrypted images: The randomness of the encrypted images is a crucial parameter that shows whether the proposed RDH scheme adversely affects the efficiency of the image encryption process. We have used a well-known encryption process. Entropy and histogram analysis are two well-known ways to analyze the efficiency of image encryption. The entropy is defined as follows:

$$Entropy = -\sum_{n=0}^{L-1} P_n \log_2 P_n \tag{5}$$

where n indicates the gray levels and P_n indicates the probability with respect to the gray level n. We do not have any control over the entropy of the original image. But the entropy measure after RDH through the encryption process is expected to get a value near 8. Similarly, the histogram of the original image will have its own shape, and it depends only on the pixel distribution in the original image. But the histogram of the encrypted to the flat due to uniform distribution of pixels in the encrypted image.

The entropy and histogram analysis has been used for verifying the randomness in the encrypted images.

The entropy from the original image and the entropy from the encrypted images are given in Table IV.

TABLE IV. ANALYSIS OF ENTROPY AFTER IMAGE ENCRYPTION

Image name	Entropy from original image	Entropy from encrypted image
Natural Images		
Baboon	7.3583	7.9992
Airplane	6.7025	7.9993
Peppers	7.5973	7.9994
Boat	7.1914	7.9993
Medical Images		
Medical image 1	6.0235	7.986
Medical image 2	5.1903	7.9687
Medical image 3	4.6429	7.9692
Medical image 4	4.3400	7.9553

From Table IV, it can be seen that all the encrypted images have an entropy of 7.999 which means all those have a very high amount of randomness.

The histograms of the original image and the corresponding encrypted image are given in Fig. 5 and Fig. 6. From this, it can be viewed that the histogram of the encrypted images look flat and it indicates the proposed scheme generates encrypted image with uniform distribution of pixels.

C. Analysis of image Recoverability

Image recoverability: This is a crucial parameter of any RDH scheme. This checks the quality of image recoverability. As per the definition of RDH schemes, we are expecting the exact recovery of the image at the receiver side after data extraction. Two parameters called Peak Signal to Noise Ratio (PSNR), and Structural

Similarity Index (SSIM) are popularly used to compare the image recoverability of an RDH scheme. These two measures are basically known as reference image quality measures. If the original image and recovered are exactly the same, then we will get ∞ as PSNR value and 1 as SSIM measure.

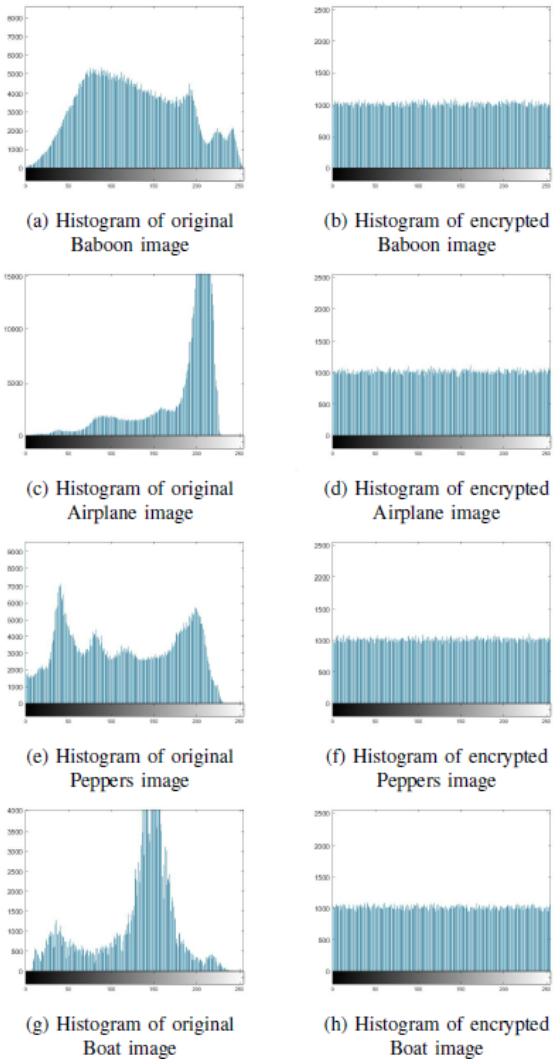

Figure 5. Histogram analysis of proposed scheme on the natural images.

The PSNR and SSIM measures are used to find the image recoverability from the proposed scheme. The PSNR and SSIM measures observed during the experimental study are given in Table V. The results claim that all those images were recovered correctly during the experimental study, and hence we observed the PSNR of ∞ and SSIM of 1.

TABLE V. PSNR AND SSIM MEASURES AFTER IMAGE RECOVERY

Image name	PSNR (in dB)	SSIM
Natural Images		
Baboon	∞	1
Airplane	∞	1
Peppers	∞	1
Boat	∞	1
Medical Images		
Medical image 1	∞	1
Medical image 2	∞	1
Medical image 3	∞	1
Medical image 4	∞	1

D. Comparative Study

The embedding rate from the proposed scheme is compared with the existing schemes in Table VI.

TABLE VI. COMPARISON OF EMBEDDING RATE

Image name	Embedding rate (bits per pixels)
Scheme in [25] 0.0039	Scheme in [25] 0.0039
Scheme in [19] < 0:0468	Scheme in [19] < 0:0468
Scheme in [15] < 0:0156	Scheme in [15] < 0:0156
Scheme in [16] < 0:0156	Scheme in [16] < 0:0156
Scheme in [17] < 0:0468	Scheme in [17] < 0:0468
Scheme in [19] < 0:0468	Scheme in [19] < 0:0468
Proposed scheme 0.0539	Proposed scheme 0.0539

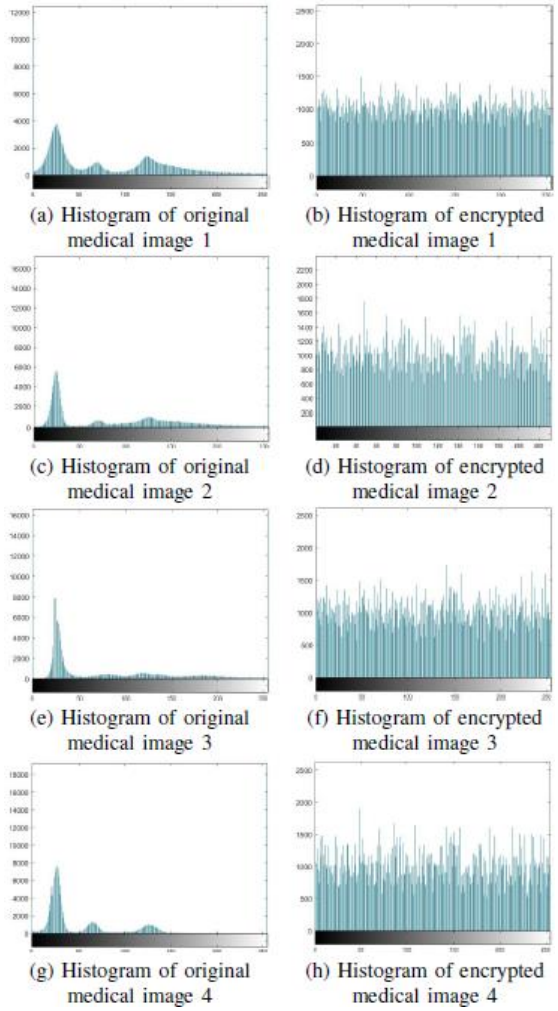

Figure 6. Histogram analysis of proposed scheme on medical images.

V. CONCLUSION

A reversible data hiding through encryption scheme that uses advanced encryption standards for image encryption with a key scrambling approach is introduced in this manuscript. This method of RDH performs data

embedding during the process of encryption. We have performed encryption using the Advanced Encryption Standard (AES) algorithm and used one of the well-known image scrambling techniques, Arnold transform, for key scrambling. In the proposed scheme, the image will be encrypted block wise and each block is used to embed a certain number of bits from the text data. The proposed scheme is mainly introduced to be used in the healthcare domain to transmit medical images in encrypted form, and the additional clinical reports can be embedded in the medical image itself. The proposed scheme has experimented on natural and medical images, and we have observed an embedding rate of 0.0539 bits per pixel which is much higher than the embedding rate from the state-of-the-art approaches. In our future works, we plan to reduce the image encryption and decryption time which are currently very high in the proposed scheme.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHOR CONTRIBUTIONS

Mr. Kandala Sree Rama Murthy designed the proposed scheme discussed in this manuscript. He also implemented the proposed scheme using Matlab, collected and analyzed all the experimental results. Dr. V. M. Manikandan has validated the experimental results. He also contributed while drafting the manuscript and doing the final proofreading; all authors had approved the final version.

ACKNOWLEDGMENT

The authors are thankful to the SRM University-AP for all the support received to complete this research work

REFERENCES

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, 2007.
[2] M. Khan and T. Shah, "A literature review on image encryption techniques," *3D Research*, vol. 5, no. 4, pp. 1-25, 2014.
[3] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003.
[4] Y. Q. Shi, Z. Ni, D. Zou, C. Liang, and G. Xuan, "Lossless data hiding: fundamentals, algorithms and applications," in *Proc. IEEE International Symposium on Circuits and Systems*, 2004, vol. 2.
[5] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: An overview and a classification," *EURASIP Journal on Information Security*, vol. 2010, pp. 1-19, 2010.
[6] C. C. Chang, T. D. Kieu, and Y. C. Chou, "A high payload steganographic scheme based on (7, 4) hamming code for digital images," in *Proc. International Symposium on Electronic Commerce and Security*, 2008, pp. 16-21.
[7] X. Li, B. Li, B. Yang, and T. Zeng, "General framework to histogram-shifting-based reversible data hiding," *IEEE Transactions on Image Processing*, vol. 22, no. 6, pp. 2181-2191, 2013.
[8] W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression," *IEEE Transactions on Image Processing*, vol. 22, no. 7, pp. 2775-2785, 2013.
[9] J. Y. Hsiao, Z. Y. Lin, and P. Y. Chen, "Reversible data hiding based on pairwise prediction-error histogram," *Journal of Information Science & Engineering*, vol. 33, no. 2, 2017.
[10] A. Malik, H. X. Wang, Y. Chen, and A. N. Khan, "A reversible data hiding in encrypted image based on prediction-error estimation and location map," *Multimedia Tools and Applications*, pp. 1-24, 2020.
[11] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255-258, 2011.
[12] S. Yi and Y. Zhou, "Binary-Block embedding for reversible data hiding in encrypted images," *Signal Processing*, vol. 133, pp. 40-51, 2017.
[13] S. Yi and Y. Zhou, "Parametric reversible data hiding in encrypted images using adaptive bit-level data embedding and checkerboard based prediction," *Signal Processing*, vol. 150, pp. 171-182, 2018.
[14] C. Qin, W. Zhang, F. Cao, X. Zhang, and C. C. Chang, "Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection," *Signal Processing*, vol. 153, pp. 109-122, 2018.
[15] V. Manikandan and V. Masilamani, "Reversible data hiding scheme during encryption using machine learning," *Procedia Computer Science*, vol. 133, pp. 348-356, 2018.
[16] V. Manikandan and V. Masilamani, "A novel entropy-based reversible data hiding during encryption," in *Proc. IEEE 1st International Conference on Energy, Systems and Information Processing*, 2019, pp. 1-6.
[17] V. M. Manikandan and V. Masilamani, "An improved reversible data hiding scheme through novel encryption," in *Proc. Conference on Next Generation Computing Applications*, 2019, pp. 1-5.
[18] V. Manikandan and A. Bini, "An improved reversible data hiding through encryption scheme with block prechecking," *Procedia Computer Science*, vol. 171, pp. 951-958, 2020.
[19] V. Manikandan, "A reversible data hiding scheme through encryption using rotated stream cipher," *Computer Science*, vol. 22, no. 2, 2021.
[20] S. M. Wadi and N. Zainal, "High definition image encryption algorithm based on AES modification," *Wireless Personal Communications*, vol. 79, no. 2, pp. 811-829, 2014.
[21] W. Chen, C. Quan, and C. Tay, "Optical color image encryption based on Arnold transform and interference method," *Optics Communications*, vol. 282, no. 18, pp. 3680-3685, 2009.
[22] M. R. Abuturab, "Securing color information using Arnold transform in Gyrator transform domain," *Optics and Lasers in Engineering*, vol. 50, no. 5, pp. 772-779, 2012.
[23] USC. Image database. [Online]. Available: http://sipi.usc.edu/database/
[24] The Cancer Genome Atlas Lung Adenocarcinoma Collection (TCGA-LUAD). [Online]. Available: https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=6881474
[25] S. Agrawal and M. Kumar, "Mean value based reversible data hiding in encrypted images," *Optik*, vol. 130, pp. 922-934, 2017.

Dr. V. M. Manikandan is currently working as an Asst. Professor in Computer Science and Engineering at SRM University-AP, Andhra Pradesh, India. He did his Ph.D. in Computer Engineering from the Indian Institute of Information Technology Design and Manufacturing Kanchipuram, Chennai, Tamilnadu, India, after his M.Tech in Software Engineering from Cochin University of Science and Technology, Kerala, India. He is an Associate Member of The Institution of Engineers (India). His research interests include reversible data hiding, digital watermarking, and digital image forensics.

Mr. Kandala Sree Rama Murthy is currently doing his B.Tech in Computer Science and Engineering at SRM University-AP, Andhra Pradesh, India. His research interests include designing and implementing digital image processing algorithms and machine learning.