EAI Endorsed Transactions
on Pervasive Health and Technology
Research Article EAI.EU

Hybrid Robust Image Steganography approach for the secure transmission of biomedical images in Cloud

Arunkumar S[1], Subramaniyaswamy V[1,*] and Logesh R[2]

[1]School of Computing, SASTRA Deemed University, Thanjavur, Tamilnadu, India.
[2]Sri Ramachandra Faculty of Engineering and Technology, Sri Ramachandra Institute of Higher Education and Research, Chennai, India

Abstract

INTRODUCTION: A rich patient may reside in their home and may prefer to take treatment with all the medical appliances inside the premise. A patient may take treatment in the less specialized hospital, which may be taking a suggestion from a specialist working in a specialized center. In such a scenario, bio-medical images need to be transmitted over the public network. Bio-medical images sent in plain form suffer from confidentiality and integrity problem.

OBJECTIVES: To overcome the above problem, medical records are always hidden in the cover image so that others do not know what is being sent.

METHODS: In our proposed scheme, the chosen cover image gets divided into the following three planes, namely: R plane, G plane, and B plane. The co-occurrence matrix is computed for each plane by dividing it into 16 x 16 pixels block and then the embedding map is generated from it. The biomedical image is also divided into 8 x 8 pixels block and is hidden into the chosen cover image block using the embedding map. Both cover image blocks and secret image blocks are transformed by RIWT. R matrix of QR decomposition of the cover image and secret image blocks are used in embedding At the end of the embedding phase. These three planes are merged into an RGB image to produce a stego image.

RESULTS: To assess the performance of our scheme, parameters like imperceptibility, robustness, and security are considered. With respect to imperceptibility, PSNR values of the stego images are over 50. With respect to robustness, average NCC values between the original secret and the attacked secret is 0.94. With respect to security, stego image cannot be detected easily if it has any secret.

CONCLUSION: From the experimental results, our scheme is proved to be better with respect to these three selected parameters.

Keywords: Image Steganography, biomedical images, secure transmission, Cloud, QR Decomposition.

Received on 28 February 2019, accepted on 05 April 2019, published on 15 May 2019

doi: 10.4108/eai.13-7-2018.162401

*Corresponding author Email: vsubramaniyaswamy@gmail.com

1. Introduction

This new-age technology that uses information and communication has been developing health care in many ways. Nowadays, electronic medical prescriptions are provided to patients by medical professionals, and wireless media is used to exchange medical information. Medical data is transmitted between hospitals for inferring the diagnostic outcomes and communicating to study a therapeutic case [1]. Telemedicine is defined as that method that uses telecommunication along with information technology for the provision of health care from a distance. This method has helped conquer several hurdles like distance barriers and improved access to these medical services that were initially not within easy reach for communities belonging to the distant rural[2]. Telemedicine is considered the best in the healing of a brain tumour. A brain tumour can be defined as a mass present in the brain that is formed when brain cells divide and multiply at an exponential rate. Tumours are found to originate from the cells present in the brain and can end up being harmful to the cells on the application of extreme pressure. [3].These tumours in the brain grow at a rapid pace. It grows to double its original size in just a span of twenty-five days. If it is not attended immediately, the patient may not live longer than half a year. As experts in this area are less and are working only in major cities, the medical data of a patient suffering from a brain tumour in remote areas is sent to experts in super-speciality hospitals for further analysis and treatment as shown in fig.1 [4].

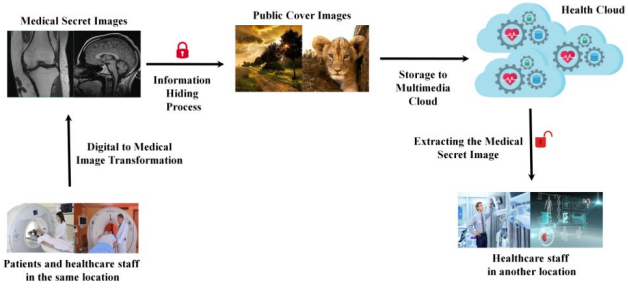


Fig. 1. Transmission of the bio-medical image between hospitals

These telemedicine platforms possess a high probability of getting caught amidst a web of risks that include intentional or unintentional manipulation of data regarding the personal information, diagnosis and prescriptions of the patients, which may lead to improvement of the disease and cause death[5]. At a cybersecurity conference held in 2011 by Black Hat, a man diagnosed with diabetes demonstrated how it is possible for someone to tap into a wireless insulin pump [6]. Medical data are sensitive information that should be protected before they are transmitted or stored. In the healthcare, security means protecting the healthcare data from being accessed by unauthorized personnel during transport or while stored in a place and privacy means assurance that only those who possess complete authorization can access and view the data. Privacy and security of patient's medical data are crucial [7].

The several methodologies available to hold a patient's information confidential can be classified under these two sub-categories. Methods that primarily deal with encryption and cryptographic algorithms will fall under the first category. In this technique, the data is secured during communication and stored in a complicated encrypted format. One main disadvantage of this technique is it requires large computational power [8]. The second technique is steganography. Steganography is data hidden within data. It is also termed as the art and science of keeping sensitive information in a secret manner such that unless one belongs to the team of personnel who are aware of how to decode the secret, you will be unable to decode or detect. One advantage that comes with steganography is that, if executed well, all the viewers are found to be extremely oblivious to the changes implemented. These steganographic techniques can be applied to images, video files or even audio files[9]. The quantum hiding technique is used to share medical images between two hospitals that are distant. Healthcare staff from one hospital uses this technique to keep significant information hidden (eg.images) and send images that are publically covered to the cloud. The healthcare staff from the other hospital, retrieve these images from the cloud and recover using several extraction procedures [10].

At the initial stage of steganography, any image was considered as the cover image for hiding a secret without considering the statistical property like a smooth surface, similarity feature or contrast

feature. But these features play an important role in determining the imperceptibility of hidden cover or the stego image quality. So, embedding process starts, the chosen cover image is subjected to measuring value for the above-said feature to increase both imperceptibility of hidden cover and the stego image quality[11]. For identifying a feature of a cover image, a grey level co-occurrence matrix(GLCM) can be constructed. This measure is calculated by the special interaction of one pixel with the rest of the pixel in a particular direction, say, in the horizontal direction or vertical direction or both [12]. Steganalysis is the method that involves the extraction of embedded secret from the stego image without the knowledge either of key or location where the secret is embedded. Identifying proper embedding locations in the cover image has a profound effect on confusing steganalysers. If location is arbitrary and cannot be predicted, then extraction by steganalyser becomes a tough process. Due to these merits, our approach selects a proper location in a cover image by measuring features to hide our secret image.

SVM was used as a major tool for performing Steganalysis on the stego images. But recently deep learning-based approaches have started to emerge for Steganalysis. Here, absolute values of elements in the feature maps are generated from the initial layer of convolution which are later propagated to the deeper layer to improve statistical modelling. This results in better performance in the detection of the existence of the secret in the stego image [13]. To improve classification efficiency further, the output of the initial layer of convolution is feed into the Quantization and truncation phase which then takes its output into the subsequent layer. An increase in detection ratio is proved experimentally and is cost-effective also [14].

In our proposed scheme, a secret medical image which needs to be sent to super specialty centres are encrypted using an image encryption algorithm. Then a suitable cover image is chosen and is then split into three planes, R plane, G plane, and B plane. The secret image is distributed into all three planes according to the values of the co-occurrence matrix which is calculated using the block selection algorithm. At the end of the embedding phase, these three planes are merged into an RGB image to produce a stego image. Obtained stego image is then sent to super speciality centres for further processing. Extract of the confidential medical image from the stego images follows a similar approach.

The organization of this article is as follows. Section 2 delineates related articles in the literature, and section 3 refers to our proposed methods, Section 4 analyzes the performance evaluation of the suggested methods, and at last Section 5 concludes our research finding and provides future direction.

2. Literature Survey

Virtual monitoring and evaluation of one's health in their own homes is the primary question of this article. Research areas that use an amalgamation of IoT and CC for healthcare have been very active. An intricate structure that encompasses various health ecosystems, extracts data from the sensors and is watermarked for safety purposes and is conveyed to the cloud for feature classification and extraction is analyzed [15]. One-class aid vector machine is used to classify an ECG as normal or abnormal. A structure that preserves private data and facilitates secure transmission is presented in [16]. Overexploitation of Boudly components for movable healthcare systems such as wheelchairs is analyzed in[17]. The model discussed in[18]intends to accomplish the diagnosis of illnesses that occur constantly such as Diabetes. Patient-related data is acquired through sensors attached to the body and is reserved into the cloud for further study and categorization. Less amount of energy is consumed in this client-server prototype. The architecture discussed in [19] data is sent to the cloud by means of a home gateway. It is processed and made available for professionals in the field and for patients. This procedure is not well explained, but our work complements these works in several ways. The PPHM is a three-layered integrated approach which is developed based on cloud and body-sensor-network (BSN) called Body-cloud. In body-cloud architecture, sensors are attached to a patient who may stay in his comfortable place which may be a small hospital near his home or in his home itself. Sensors capture images and then transmit to the cloud server for further processing. This model allows a healthcare professional with the basic authorization to acquire real-time data accumulated by a sensor in an IoT subsystem [20]. As of now, research scientists are focussed on the usage of methods involving cryptography and watermarking schemes licensing an optimal balance between safety and durability in

telemedicine applications [21]. Research has proven that spatial domains are less immune to attacks than transform-based techniques [22].Nevertheless, watermarking based on spatial domains consumes less time than techniques that embed information into the transform domain. Of late, DWT has emerged as a more efficient alternative as a transform domain technique amongst others. Although, poor directional data and shift variant is the major primary concerns when it comes to DWT. Shift-variant may be avoided by using RDWT [23] but it does not render rich directional information. Multiple watermarking amplify security and reduces the necessity of storage and bandwidth while transmission. It also overcomes the problems faced by the management of health data while embedding less strong watermark information at a much lower decomposition degree and stronger watermark at higher levels of decomposition [24,37]. To embed binary watermark of size 15*64 that uses an encryption key, an algorithm was proposed for varied color spaces that use Arnold Transform Mapping and DWT[25]. A combined technique of Arnold's Transform Map and Cross Chaos Map for the embedding of watermark[26] was proposed using the coefficients of DCT. An algorithm proving proof that higher sub-bands give less robust results in comparison to LL sub-band was put forward by Fan et al. Using nature images, LL is experimentally determined to be the smooth region by conducting tests over approximate sub-band coefficients [27]. An idea for watermarking, using Hadamard Transform Technique and entropy method as a basis, was put forward by Franklin et al., where the host image is split into 8*8 sized blocks and embedding of the watermark is done in those blocks which are calculated to have higher entropy values [28]. Using YIQ color space and the IWT basis, another watermarking scheme was put forward by Yang et al. IWT can map integer to integer accurately, and YIQ color space gives an understanding about the brightness. Yet another algorithm was put forward with PCA as a basis [29]. In the JPEG domain, feature set proposed in DCTR [30] is the combined advantages of low dimensionality and competitive performance. At the same tile steganalysis proposed in PHARM [31] and GFR [32] demonstrate better performance with a higher cost of dimensionality regard to DCTR. Steganalysis proposed in [33] is a slight variation of selection-channel-aware of JPEG rich models targeted at content-adaptive JPEG steganography.

3. Proposed Methodologies

In this section, the Hybrid Robust Image Steganography scheme is proposed to secure the transmission of biomedical images. Biomedical images are encrypted using the logistic chaotic map to translate it to the cipher image. Cipher image is segmented into blocks of 8 x 8 pixels. An RGB cover image is chosen to hide our biomedical images. The selected cover image is separated into three image planes. Each plane is segmented into blocks of 16 x 16 pixels separately. The co-occurrence matrix is measured for every block of all three planes and according to its value, DCT, RIWT is applied on that particular block of a plane and then embedding is done. From this, the embedding map is calculated which is sent to the receiver side. QR decomposition is applied both on RIWT transformed blocks of cover image planes and on encrypted secret image blocks. The proposed method consists of three sections, section 3.1 explains the embedding distortion measure (EMD), section 3.2 explains the embedding phase and section 3.3 explains the extraction phase of our method.

3.1 Embedding Distortion Measure

A co-occurrence matrix is computed for each block in all the three R, G and B planes of a cover image. [11] explains the cover selection algorithm for selecting the best cover among the pool of covers from the image database. The above method is slightly modified to suit our requirement in our proposed algorithm as follows. Following steps are applied for every block of the cover image to obtain the co-occurrence matrix by using the relationship between every pixel,

Pseudo code for Embedding Distortion Measure	
Input: $M \times N$ sized Cover image	
Output: co-occurrence matrix C (x, y)	
Step 1:	Compute co-occurrence matrix C (x, y) by calculating how often pixel value x occurs horizontally adjacent to a pixel with value y. The number of unique pixel value

determines the size of the co-occurrence matrix

Step 2: Compute contrast as follows,

$$\sum_{i,j} |i-j|^2 p(i,j)$$

Step 3: Compute correlation as follows,

$$\sum_{i,j} \frac{(i-\mu_i)(j-\mu_j)p(i,j)}{\sigma_i \sigma_j}$$

Step 4: Compute the number of cover image block necessary to embed

Step 5: Set the threshold value for both contrast and correlation values.

Step 6: Compare values of contrast and correlation of each block with its respective threshold value.

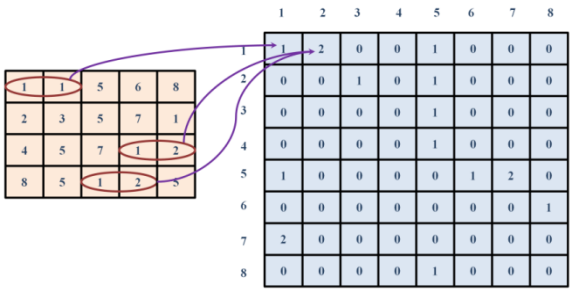


Fig. 2. Co-occurrence matrix

By extracting features from the computed co-occurrence matrix, block with high contrast is chosen amongst three planes for each block as shown in fig.3. The secret image block is hidden on to the chosen cover image block. For hiding, the cover image block is first transformed by RIWT and then by DCT to produce coefficient. QR decomposition is applied to both the secret image block and cover image block. R component of the secret image block is embedded into R component of the cover image block.

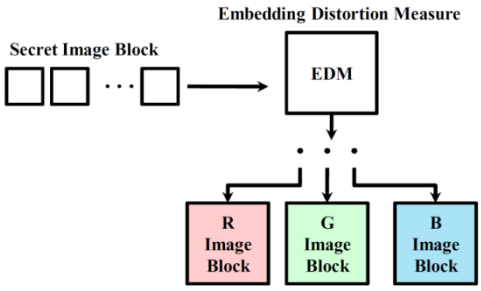


Fig. 3: Embedding Distortion Measure

3.2 Embedding Phase

Let C be Color Image of size 512 x 512 pixels are treated as a cover image. C is first divided into three planes: R plane, G plane, and B plane. Each plane is decomposed into blocks of 16 x 16 pixels. The secret image I of size 256 x 256 pixels is encrypted using a logistic chaotic map and then is decomposed into blocks of 8 x 8 pixels. Embedding Distortion Measure is applied on each block of three planes against blocks of secret image blocks which produces three stego image planes. All three stego image planes are merged to produce a stego image. Figure 4 shows the embedding phase and is explained as below,

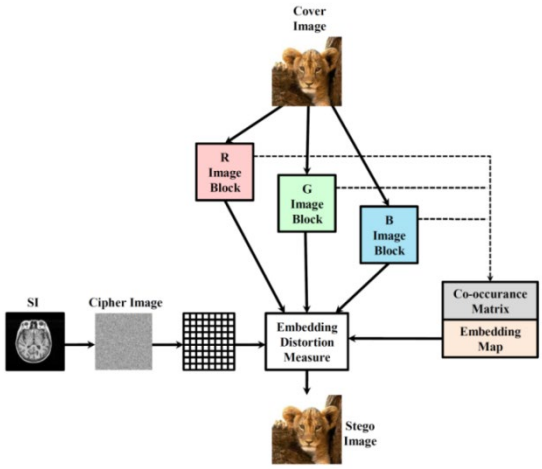


Fig. 4. Architectural diagram for embedding phase.

Pseudo code for Embedding Phase

Input: Cover image of size of 512 x 512, Secret image of size 256 x 256

Output: Stego image of 512 x 512, Embedding Map

Step 1: Divide the cover image into three planes: R plane, G plane, and B plane

Step 2: Decompose the cover image into 16 x 16 pixels block. RB_i, GB_i, BB_i represents the i^{th} cover image block of Red, Green and Blue plane(Generically it is called CB_i while performing embedding).

Step 3: Compute co-occurrence matrix for CB_i.

Step 4: Generate embedding map according to the co-occurrence.

Step 5: Encrypt the secret image S using logistic chaotic map to obtain S1.

Step 6: Decompose the cipher secret image S1 into 8 x 8 pixels block into SB_i

Step 7: Perform the following steps on CB_i whose value is 1 in embedding map

7.1 Perform 1-level RIWT on the block CB_i followed by DCT transform

7.2 Apply QR both to CB_i and SB_i

7.3 Embed secret image block's R matrix into cover image's R matrix using the scaling factor α as follows,

$$R^1_i = RCB_i + \alpha \times RSB_i .$$

7.4 Apply inverse of the above step as follows to obtain modified coefficient matrix SB_i,

Inverse of QR (sub-band of CB_i) = QCB_i x R^1CB_i

7.5 Apply inverse of transform by combining modified sub-band and the other three sub-bands to obtain stego image block SB_i.

Step 8: Merge all SB_i to obtain stego image.

3.3 Extraction Phase

Stego image is divided into three planes R, G and B planes. Each plane is decomposed into blocks of 16 x 16 pixels. Based on the value of the embedding map, these three planes are transformed using RIWT and also by DCT. QR factorization is done on LL to get the R matrix. The R matrix produced in the embedding phase is utilized to obtain an encrypted secret image block. Then, all blocks are concatenated to obtain a secret image and are then decrypted using the logistic chaotic map to extract the secret image. The extraction phase is explained as below,

Pseudo code for Extraction Phase

Input: Stego image of size 512 x 512, QC_i, RI_i, and embedding map
Output: Secret image I of size 256 x 256

Step 1: Split the stego image S to R, G and B planes.

Step 2: Decompose S into 16 x 16 pixels blocks. SB_i is the i^{th} block of stego image

Step 3: Perform the below steps for all block whose value is 1 in embedding map

3.1 Transform SB_i using 1-level RIWT and transform the desired sub-bands by DCT.

3.2 Apply QR to SB_i using QR (SB_i) = QI_i x RI_i

3.3 Extract secret image block JB_i using $R^2i = (R^1I_i - RI_i) / \alpha$

3.4 Apply inverse of QR to get coefficient JBi as JBi = QC_i x R^2i

Step 4: Merge entire blocks of JBi to obtain J.

Step 5: Perform inverse of logistic chaotic map on J to get the embedded image .

4. Experimental result and analysis

MATLAB R2017b is used for performing the simulation of the results. Imperceptibility, resistance to steganalysis, and robustness are the

metric used to analyze the scheme for effectiveness and are discussed in section 4.1, 4.2, and 4.3, respectively. The result of the scheme is compared with the related methods in section 4.4.

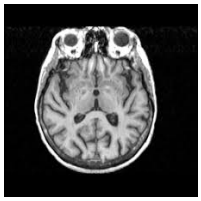
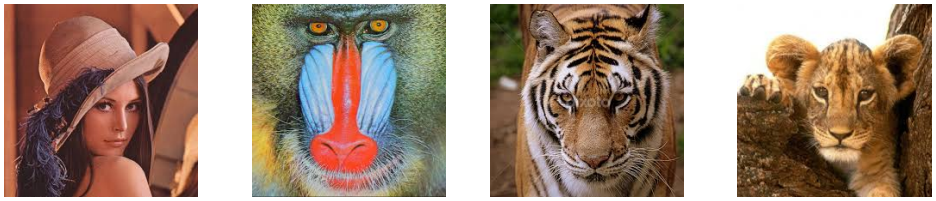
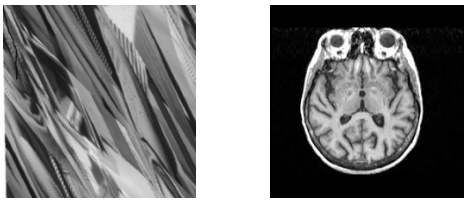


Fig. 5. Secret image



(a) Lena (b) Baboon (c) Tiger (d) Cat

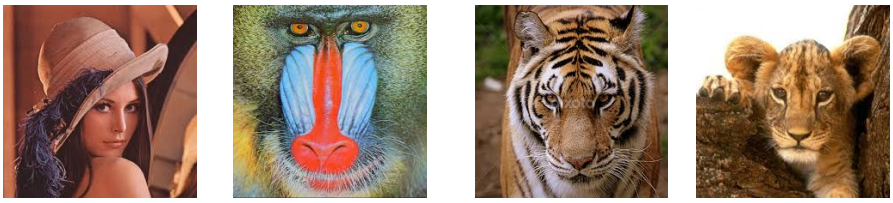
Fig. 6. Cover images



(a) Extracted image using the wrong key

(b) Extracted image using the correct key

Fig. 7. Extracted image



PSNR= 52.33 MSSIM= 0.9883 NAE= 0.0015 IF= 1.0	PSNR= 53.27 MSSIM= 0.9898 NAE= 0.0022 IF= 0.9998	PSNR= 52.67 MSSIM= 0.9943 NAE= 0.0017 IF= 0.9997	PSNR= 52.62 MSSIM= 0.9886 NAE= 0.0019 IF= 0.9997

Fig. 8. Imperceptibility property of the scheme

4.1 Imperceptibility

PSNR, MSSIM, NAE and IF are the metric used to assess the imperceptibility which is the measure of the amount of invisibility of the existence of a secret image in the resultant image.

The secret image depicted in Fig 5 is hidden into the images shown in Fig.6. Secret image is subjected to encryption which is done to provide better security. Without the proper decryption key, extraction cannot be completed properly, even if the extraction algorithm is known. Fig.7(a) shows the obtained stego image through the wrong key, Fig.7.(b) shows the obtained stego image through the correct key. The stego image produced by the embedding is shown in Fig.8.

Stego images depicted in Fig.8 provide more PSNR values ranging between 53.62 and 53.76. The above values are more than the values produced by a similar scheme of the literature. MSSIM and IF values for all the stego images are close to 1, which is the desired value. The NAE value is almost zero, that is the required value. From the above values, It is inferred that the scheme produces a better stego image.

4.2 Resistance to Steganalysis

Deep learning-based Steganalysis scheme discussed in [13] which is without the Q&T phase and [14] which is based on a hybrid deep learning approach with the Q&T phase integrated into it is used here for assessing the strength of stego image produced by our proposed scheme. Features of the image are extracted and are used to classify if a candidate image is a stego image or innocent cover image. The procedure used for classification can be split into three phases,

1) *Convolution*: Convolution uses a set of kernels on the target image to produce a diverse noise residual. Convolution smoothens out some of the image contents and also helps to increase the Signal-to-Noise Ratio(SNR).

2) Quantization and truncation (Q&T): Each residual is quantized on a different scale and is truncated to enhance the identity of the individual feature set, as well as to reduce the complexity in the computation.

3) *Aggregation*: Noise residual values are collected to decrease the dimensionality of features.

The detection accuracy of [13] is 54.7% which is better than the SVM based classifier. But the detection accuracy of [14] is 74.5% which is better than both SVM and traditional deep learning-based approach. An increase in the detection ratio is contributed to the presence of the Q&T phase. Even in this Q&T phase, if only with truncation, its ratio is 57.6%, and with only quantization is 65.4%. If both quantization and truncation are used, then its ratio is better. We can easily infer that both quantization and truncation effectively improve the detection performance as can be seen in table 1.

Table 1. Steganalysis results for Deep learning-based approaches

Deep learning approach	[13]	[14]
Without Truncation & Quantization	54.7%	-
With Truncation only	-	57.6%,
With Quantization only	-	65.4%.
With both Truncation & Quantization		74.5%

4.3 Robustness

Robustness is the ability to fish-out the embedded secret image properly from the stego image that was under attack. It is measured using the Normalized Cross-Correlation (NCC) values. It gauges the resemblance between the original and the extracted secret image. The produced stego images are subjected to various image processing attacks, as shown in Fig.9.

The secret image is extracted properly from all attacked stego images. NCC is computed between the original and the extracted secret images, as shown in Table 2. This table shows, NCC value are close to 1 which is the desired result. It is concluded that the method is robust enough to stay immune to image processing attacks.

Table 2. NCC values of extracted secret image from stego images subjected to various attacks.

Attacks	Lena	Baboon	Tiger	Cat
	NCC	NCC	NCC	NCC
Resize [1024 1024]	0.9831	0.9707	0.9776	0.9867
Rotate 15^0	0.9432	0.9532	0.9624	0.9847
Sharpen	0.8759	0.8951	0.9179	0.8676
Blur	0.9975	0.9874	0.9938	0.9743
Salt & pepper noise with density 0.001	0.9018	0.8745	0.9182	0.8693
Gaussian noise with variance 0.001	0.9427	0.9381	0.9673	0.9638

(a) Resize [1024 2014]

(b) Rotate 15^0

(c) Sharpen

(d) Blur

(e) Gaussian noise with variance of 0.001

(f) Salt & pepper noise with variance of 0.001

Fig. 9. Stego images set under various attacks

4.4 Comparison with similar schemes

PSNR values of our experimental results are compared with other related schemes like Ghebleh et al, Hu et al and Rabie et al as shown in Table 3. The NCC results between both the original and extracted secret image from our scheme for nearly all the nine parameters like Gaussian noise, etc., is superior over the other three schemes. Results obtained after experimenting in Table 3 proves the dominance of this scheme.

Table 3. Comparison of PSNR values of our scheme with other three related schemes

Schemes / Cover image	Ghebleh et al	Hu et al	Rabie et al	Ours
Lena	51.93	48.69	45.40	53.33
Baboon	51.48	49.66	45.12	52.27
Tiger	52.05	51.86	46.78	53.67
Cat	53.19	48.73	45.04	54.62

5. Conclusion

An efficient image steganographic scheme to ensure the secure transmission of patients confidential details is devised. It is devised using on RIWT, DCT, and QR. The method has exploited the merits of technology like RIWT, DCT, the QR decomposition technique, and the logistic chaotic map to achieve the aim. RIWT is a shift-invariant, which makes the scheme more reversible and robust. DCT is used to achieve increased imperceptibility by embedding in medium frequency subbands only. The logistic chaotic map is used to encrypt secret images which provide extra security and QR improves the robustness of our scheme. Embedding is performed on a LL sub-band of the QR decomposed block, steganalysis has become a difficult activity. In addition to it, changes effected on the R matrix of QR efficiently withstand the attacks by image manipulation. The results of experimentation, its subsequent analysis and the comparison of results of the scheme with similar schemes in the literature, prove that the patient's confidential details can be transmitted to any recipient with utmost confidence. We propose to enhance the scheme to transfer the patient's USG and Doppler report, which are multicolor in nature, to any recipient securely, as the future work.

References

[1] Chakraborty, S., Samanta, S., Biswas, D., Dey, N., & Chaudhuri, S. S. (2013, December). Particle swarm optimization based parameter optimization technique in medical information hiding. In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on (pp. 1-6). IEEE.

[2] Traver, V., Monton, E., Bayo, J. L., Garcia, J. M., Hernandez, J., & Guillen, S. (2003). Multiagent home telecare platform for patients with cardiac diseases. Computers in Cardiology, 1(30), 117-120.

[3] Haj-Hosseini Neda , Peter Milos , Camilla Hildesj , Martin Hallbeck , Johan Richter , Karin Wrdell. (2016) . Fluorescence spectroscopy and optical coherence tomography for brain tumor detection, in: SPIE Photonics Europe, Biophotonics: Photonic Solutions for Better Health Care, Brussels Belgium, SPIE-International Society for Optical Engineering , pp. 9887–9896 .
[4] Amin, J., Sharif, M., Yasmin, M., & Fernandes, S. L. (2017). A distinctive approach in brain tumor detection and classification using MRI. Pattern Recognition Letters.
[5] Lubacz, J., Mazurczyk, W., & Szczypiorski, K. (2013). New Ways to Smuggle Messages across the Internet. IEEE Spectrum. 50(11):42–4523
[6] Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. Communications of the ACM, 58(4), 74-82.
[7] Vargheese, R., & Prabhudesai, P. (2014). Securing B2B pervasive information sharing between healthcare providers: enabling the foundation for evidence based medicine. Procedia Computer Science, 37, 525-530.
[8] Calvillo, J., Román, I., & Roa, L. M. (2013). Empowering citizens with access control mechanisms to their personal health resources. International journal of medical informatics, 82(1), 58-72.
[9] Ahmad, T., Studiawan, H., Ahmad, H. S., Ijtihadie, R. M., & Wibisono, W. (2014, October). Shared secret-based steganography for protecting medical data. In Computer, Control, Informatics and Its Applications (IC3INA), 2014 International Conference on (pp. 87-92). IEEE.
[10] El-Latif, A. A. A., Abd-El-Atty, B., Hossain, M. S., Rahman, M. A., Alamri, A., & Gupta, B. B. (2018). Efficient quantum information hiding for remote medical image sharing. IEEE Access, 6, 21075-21083.
[11] Kharrazi, M., Sencar, H. T., & Memon, N. (2006, October). Cover selection for steganographic embedding. In 2006 International Conference on Image Processing (pp. 117-120). IEEE.
[12] Haralick, R. M., & Shanmugam, K. (1973). Textural features for image classification. IEEE Transactions on systems, man, and cybernetics, (6), 610-621.
[13]Xu, G., Wu, H. Z., & Shi, Y. Q. (2016). Structural design of convolutional neural networks for steganalysis. IEEE Signal Processing Letters, 23(5), 708-712.
[14] Zeng, J., Tan, S., Li, B., & Huang, J. (2018). Large-scale jpeg image steganalysis using hybrid deep-learning framework. IEEE Transactions on Information Forensics and Security, 13(5), 1200-1214.
[15] Hossain, M. S., & Muhammad, G. (2016). Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. Computer Networks, 101, 192-202.
[16] Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X., & Luo, H. H. (2015). Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wireless Communications, 22(4), 104-112.
[17] Yang, L., Li, W., Ge, Y., Fu, X., Gravina, R., & Fortino, G. (2014). People-centric service for mHealth of wheelchair users in smart cities. In Internet of things based on smart objects(pp. 163-179). Springer, Cham.
[18] Kaur, P. D., & Chana, I. (2014). Cloud based intelligent system for delivering health care as a service. Computer methods and programs in biomedicine, 113(1), 346-359.
[19] Luo, S., & Ren, B. (2016). The monitoring and managing application of cloud computing based on Internet of Things. Computer methods and programs in biomedicine, 130, 154-161.
[20] Fortino, G., Parisi, D., Pirrone, V., & Di Fatta, G. (2014). BodyCloud: A SaaS approach for community body sensor networks. Future Generation Computer Systems, 35, 62-79.
[21] Arsalan, M., Qureshi, A. S., Khan, A., & Rajarajan, M. (2017). Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. Applied Soft Computing, 51, 168-179.
[22] Singh, A. K., Kumar, B., Singh, S. K., Ghrera, S. P., & Mohan, A. (2016). Multiple watermarking technique for securing online social network contents using back propagation neural network. Future Generation Computer Systems.
[23] Bhatnagar, G., & Raman, B. (2009). A new robust reference watermarking scheme based on DWT-SVD. Computer Standards & Interfaces, 31(5), 1002-1013.
[24] Singh, A. K., Kumar, B., Singh, G., & Mohan, A. (Eds.). (2017). Medical image watermarking: techniques and applications. Springer.
[25] Khalili, M., & Asatryan, D. (2013). Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map. IET Signal Processing, 7(3), 177-187.

[26] Pradhan, C., Saxena, V., & Bisoi, A. K. (2012). Imperceptible watermarking technique using Arnold's transform and cross chaos map in DCT Domain. International Journal of Computer Applications, 55(15).
[27] Fan, L., & Gao, T. (2009, May). A novel blind robust watermarking scheme based on statistic characteristic of wavelet domain coefficients. In 2009 International Conference on Signal Processing Systems (pp. 121-125). IEEE.
[28] Franklin, R. V., GRS, M., & Santhi, V. (2011). Entropy based robust watermarking scheme using Hadamard transformation technique. International Journal of Computer Applications, 12(9), 14-21.
[29] Ayesha, S. K., & Masilamani, V. (2015). An Imperceptible Digital Image Watermarking Technique by Compressed Watermark Using PCA. In Advances in Intelligent Informatics(pp. 287-295). Springer, Cham.
[30] Holub, V., & Fridrich, J. (2015). Low-complexity features for JPEG steganalysis using undecimated DCT. IEEE Transactions on Information Forensics and Security, 10(2), 219-228.
[31] Holub, V., & Fridrich, J. (2015, March). Phase-aware projection model for steganalysis of JPEG images. In Media Watermarking, Security, and Forensics 2015 (Vol. 9409, p. 94090T). International Society for Optics and Photonics.
[32] Song, X., Liu, F., Yang, C., Luo, X., & Zhang, Y. (2015, June). Steganalysis of adaptive JPEG steganography using 2D Gabor filters. In Proceedings of the 3rd ACM workshop on information hiding and multimedia security (pp. 15-23). ACM.
[33] Denemark, T. D., Boroumand, M., & Fridrich, J. (2016). Steganalysis features for content-adaptive JPEG steganography. IEEE Transactions on Information Forensics and Security, 11(8), 1736-1746.
[34] Ghebleh, M., and A. Kanso. "A robust chaotic algorithm for digital image steganography." Communications in Nonlinear Science and Numerical Simulation 19.6 (2014): 1898-1907.
[35] Hu, Yu-Chen, Chun-Chi Lo, and Wu-Lin Chen. "Probability-based reversible image authentication scheme for image demosaicking." Future Generation Computer Systems 62 (2016): 92-103.
[36] Rabie, Tamer, Mohammed Baziyad, and Ibrahim Kamel. "Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid." Multimedia Tools and Applications (2018): 1-26.
[37] Arunkumar, S., Subramaniyaswamy, V., Vijayakumar, V., Chilamkurti, N., & Logesh, R. (2019). SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. Measurement, 139, 426-437.