




---

# Secure transmission and integrity verification of color radiological images using fast discrete curvelet transform and compressive sensing

Surekha Borra <sup>a</sup>  , Rohit Thanki <sup>b</sup> , Nilanjan Dey <sup>c</sup> , Komal Borisagar <sup>d</sup> 

Show more 

 Share  Cite

---

<https://doi.org/10.1016/j.smhl.2018.02.001> 

[Get rights and content](#) 

---

## Abstract

Rapid growth in digitization and globalization has influenced the medical field immensely. The radiological pictures are frequently shared comprehensively among specialists, medicinal experts, radiologists, analysts, and patients themselves by means of wired or remote media for purposes, for example, common accessibility and enhancing the diagnostic results. This paper proposes a hybrid and high capacity image hiding technique for secure transmission and integrity of color radiological images. The Compressive Sensing (CS) theory is used to encrypt the color secret image before embedding them into high frequency Fast Discrete Curvelet Transform (FDCuT) coefficients of color radiological images. The simulations gave a PSNR of 63.96 dB, which demonstrates better performance in terms of imperceptibility of stego color radiological image. Further, expansive payload limit is permitted when contrasted with many existing strategies.

---

## Introduction

Today, transmission and sharing of medicinal information over web has turned out to be exceptionally basic among the medical practitioners, diagnostic centers, hospitals, health insurance, and Telemedicine companies (Das et al., 2012, Dey et al., 2012a, Dey et al., 2012b, Dey et al., 2012c). In

such scenarios, certain secure means of communicating the electronic patient records is required in order to meet security concerns. The studies on Web services technology suggested three mandatory requirements for medical images transmission in teleradiology: confidentiality, reliability, and availability. Since last decade, various researchers and different agencies are working on to design of various techniques, rules, and standards for security and privacy requirements of medical information in teleradiology application. The first international standard for security of medical data is developed by International Standard Organization in 2008 and whose name is ISO 27799:2008 (ISO 27799:2016, 2016). In 2016, this standard is revised and is used for security management of medical data. This standard characterized diverse security and quality parameters for different sorts of medicinal information like medical images, medical videos, and medical signals. Additionally, a few nations characterized their own particular standard for security of therapeutic information. For instance, USA has used the standard Health.

Insurance Portability and Accountability (HIPAA) (HIPAA, 1996) and Code of Federal Regulations numbers 45 (CFR 45) (CFR 45, 2010). Additionally, in 1983, American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) has made one agency by name Digital Imaging and Communication in Medicine (DICOM, 2009) for building up a standard database for medical data and guidelines for security of medical data.

To outline and actualize security mechanisms in view of accessible norms for protection and security of medicinal information, different teleradiology models are planned by the specialists. Ruotsalainen (2010) built up a standard model for online transmission and also for offline transmission. The online transmission of therapeutic information is done by means of the web and offline transmission of information is done by means of printed version, hard disk or floppy. He additionally brought up different security necessities for models utilized as a part of teleradiology applications. In any standard teleradiology model, protection and security of medicinal information are influenced at chiefly three points which are demonstrated in Fig. 1.

Security is needed in the following cases: 1. when medical data is stored at system database of hospital or data is transferred from one doctor to another doctor within a hospital. 2. When medical data is transferred from one hospital to another hospital or remote treatment house via online transmission or offline transmission. 3. The security of medical data at the remote treatment house. In all these cases, the corruption or modification of medical data is possible, which may lead to wrong diagnosis and treatment of the patient. When planning any model for teleradiology applications, the model must satisfy the different security prerequisites which are said underneath (Ruotsalainen, 2010; Baur et al., 1997):

1. All concerned points or hardware utilized as a part of the model must have the same security level.
2. At all points, authorization of doctors or users must be performed through various authenticate process and controls.

3. Authenticity, confidentiality, and integrity of all medical must be secured amid different medical sessions such as consultation, processing, management, and storage.

In light of the essential necessities of models, any teleradiology model must have three attributes: confidentiality, reliability, and availability (Ruotsalainen, 2010, Baur et al., 1997, Epstein et al., 1998). The confidentiality characteristic of the model is guarantees that exclusive validated client can get to medicinal information. The reliability characteristic of the model depends on the integrity (modification data cannot be performed by the unauthenticated user) and authenticity (authentication of medical data provides to authenticated user). The availability characteristic of the model ensures that the system access is available for all authenticated users in ordinary conditions. Often the authenticity, integrity, and security of medical data are accomplished using Cryptography, Steganography and Watermarking approaches. The steganography approach is preferred for one-to-one communication. While the general requirements of such medical image hiding techniques being high capacity, invisibility, blindness, robustness and lossless. The Steganography fails when the secret image is detected by an imposter. The watermarking techniques are primarily utilized for copyright protection of images.

These days, different kinds of medical images such as MRI, CT, and PET are widely used for better treatment and diagnosis for medical issues of a patient (Thanki et al., 2017a, Thanki et al., 2017b, Singh, 2015, Nyeem et al., 2013). In telemedicine, for better treatment and diagnosis, the medical images are transmitted to the one hospital to remote hospital with patient information. At the remote hospital side, there is a need to recover the medical image with less distortion. Also, integrity of medical images is vital at system database of hospitals. Accordingly, numerous data hiding methods are designed and implemented in view of Steganography, Cryptography, robust and fragile watermarking for medical image protection and integrity, respectively.

Many researchers (Priya et al., 2017, Thakkar and Srivastava, 2017, Thanki et al., 2017a, Thanki et al., 2017b, Singh, 2015, Yassin, 2015) were depicted and evaluated various medical images hiding techniques for telemedicine applications. In these techniques, secret information is embedding into host medical image without any changes in the medical image. These techniques are designed and implemented by using various image processing transforms and encryption methods. The image processing transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and hybridization of various transforms, and so forth are utilized for secret image hiding in the existing techniques. The different encryption strategies like Hamming code, BCH code, and so forth are utilized for security of secret data in the current methods.

Thanki et al., 2017a, Thanki et al., 2017b) analyzed various steganography techniques for security of grayscale medical images in telemedicine applications. Additionally, he proposed new steganographic strategy utilizing DCT – SVD and CS encryption strategy to beat the impediment of existing procedure (Sreedhanya & Soman, 2013) for security of medical images. These techniques are defined only for grayscale medical images. Further, they have less payload limit, and low imperceptibility. Thakkar and Srivastava (2017) proposed blind medical image hiding technique using DWT and block wise SVD. In this technique, a confidential image is inserted into the values of S

matrix of approximation wavelet coefficients of medical image. The limitation of this technique is that it is only applicable for Region of Interest (ROI) of medical image.

Nagpal, Bhushan, and Mahajan (2016) proposed medical image securing technique utilizing DWT, Artificial Neural Network (ANN), and Rivest-Shamir-Adleman (RSA). In this technique, RSA encryption is applied on secret image to get encrypted secret image, which can further be inserted into wavelet coefficients of medical image to get secure medical image. The limitation of this technique is that it has less imperceptibility. In a method proposed by Mahmood (2015), the entropy of Region of Background (ROB) of medical image is found and after that few blocks with low entropy values are used for secret image embedding. Finally, DCT is applied on these blocks to get its DCT coefficients, and these coefficients are altered for secret image using insertion using LSB or difference expansion approach.

Singh, Dave, and Mohan (2014) proposed two medical image hiding techniques using DWT, SVD, and cryptography. In this technique, authors used three distinct error correcting codes such as Hamming, Bose-Chaudhuri-Hocquenghem (BCH) and Reed-Solomon (RS) codes for encryption of secret image. This scrambled image is then inserted into detail wavelet coefficients of host medical image in wavelet based technique, and into the S matrix of host medical image in case of SVD based technique. Authors suggested that RS based encrypted image hiding technique performed superior to other two codes. Venkatram et al. (2014) proposed medical image protection technique using 2D Lifting Wavelet Transform (LWT) and SVD, where singular values of LWT wavelet sub-bands of medical image are modified according to the bits of secret image to get stego medical image. Acharjee, Ray, Chakraborty, Nath, and Dey (2014) proposed medical image hiding technique for security of biomedical videos using motion vector estimation. Chakraborty, Samanta, Biswas, Dey, and Chaudhuri (2013) proposed a medical image hiding technique using Particle Swarm Optimization (PSO). This technique is a modified version of Dey, Samanta, Yang, Das, and Chaudhuri (2013) to achieved better imperceptibility. Dey et al. (2013) has designed medical image watermarking technique using DWT and by insertion of three PN sequences into detail wavelet sub bands: LH, HL, and HH according to secret image bits. Biswas, Das, Maji, Dey, and Chaudhuri (2013) proposed a visible medical image watermarking using fuzzy logic and Harris corner detection.

Pal, Dey, Samanta, Das, and Chaudhuri (2013) proposed two approaches: even-odd shifting approach and a difference approach for color medical image security. The R channel of the medical image is modified using even-odd shifting approach, while B channel is modified using difference approach according to the secret image bits. This limitation of this technique is that the secret image is not encrypted before its hiding. Dey et al., 2012a, Dey et al., 2012b, Dey et al., 2012c gave hybrid medical image hiding technique using DCT, DWT, and SVD. The singular values of DCT coefficients of HH subband of medical image are first modified by singular value of DCT coefficients of HH subband of watermark image to get watermarked medical image. This technique too has not employed any security mechanism for encryption of medical data. Rathi and Inamdar (2012) proposed Region of Non-Interest (RONI) based medical image watermarking using LWT. In this technique, first RONI of the medical image and then wavelet coefficients of RONI is acquired using LWT. Finally, multiple secret images are inserted into the wavelet coefficients using a private key.

Kumar, Singh, Singh, and Mohan (2011) proposed medical image hiding technique using DWT and spread spectrum approach. In this technique, two PN sequences are added with horizontal and vertical wavelet coefficients of host medical image when secret image has zero bit value. The extraction of secret image bit is performed using correlation between PN sequences. Based on the correlation results, secret image bit value is extracted. Mostafa, El-Sheimy, Tolba, Abdelkader, and Elhindy (2010) proposed medical image hiding technique using DWT and cryptography. In this technique, BCH code is used for encryption of secret EPR image. The DWPT is used for extraction of wavelet subbands of host medical image. Later, two wavelet subbands are divided into non-overlapping blocks, and each block value is modified by secret bits. Huang, Fang, and Chen (2009) proposed medical image hiding using DCT. In this technique, DCT coefficients of host medical image are modified by secret image.

Many watermarking related image hiding techniques for medical image authentication at hospital or remote treatment house are presented in the literature. Block-based medical image watermarking techniques and usage of genetic algorithms for optimization is the recent trend. Methods employing error correcting codes are proposed for optimal selection of locations in images for confidential data hiding. Thanki et al., 2017a, Thanki et al., 2017b proposed medical image data hiding technique in spatial domain for medical image authentication. In this technique, simple image processing operations are used. The techniques based on spread-spectrum (Langelaar et al., 2000, Zinger et al., 2001, Domingo-Ferrer and Sebe, 2002, Malvar and Florêncio, 2003, Xuan et al., 2004) are also proposed for multi-level access and reliability of data. In 2007, Ping, Ee, and Wei (2007) proposed two methods for hiding of authentication information in medical images in two dissimilar domains: (1) Circular approach and (2) RSA encryption and decryption approach. Ho, Zhu, and Shen (2004) proposed a method for biomedical content authentication based on zero's location of Z-Transforms, Discrete Pascal transform (DPT), repetitive index modulation, and hamming codes for tamper detection.

Subsequent to surveying many medical image data hiding techniques, it is observed that most of the existing techniques are designed using DFT, DCT, DWT, SVD, and their hybridizations, and are defined only for security of grayscale medical images. In addition, these techniques have less imperceptibility and payload limits. Further, very less number of image hiding techniques are available for data integrity of color medical images. In the present scenario, the improvement of medicinal imaging advancements is accompanying medical images in color version. Also color versions of hospital logos or secret information are widely being used by the hospitals which need to be integrated with the medical images for various security purposes. Therefore, security of these color medical images is required at communication channel and system database of teleradiology model.

In this paper, an image hiding and integrity verification technique for authentication of color radiological images using Fast Discrete Curvelet Transform (FDCuT) and CS based encryption (Candes, 2006; Candes & Wakin, 2008; Zhang et al., 2016; Tropp & Gilbert, 2007) method is proposed. The proposed method contributes to security improvement by integration of CS based encryption for generation of encrypted secret images before hiding them into color radiological images. This technique is an extension of Rohit technique (Thanki & Borisagar, 2016) which was designed for

authenticity of multibiometric data. The present paper shows the application of Rohit technique (Thanki & Borisagar, 2016) for integrity of color medical images at security point 1 and point 3 of teleradiology model.

The high-frequency curvelet coefficients of host color medical image are modified according to encrypted secret image bits to generate stego color medical image. The high frequency Curvelet coefficients of host color medical image and all wavelet coefficients of color secret image are chosen to accomplish the fragility nature in the proposed technique. The Orthogonal Matching Pursuit (OMP) algorithm (Tropp & Gilbert, 2007) is used for decryption of color secret image. The reason behind using FDCuT in the proposed technique is that it overcomes the limitations of DFT, DCT, and DWT (in which large number of transform coefficients are required to hide an image) by its sparsity and directionality properties. Sparsity property of FDCuT helps in describing the image accurately using few coefficients and also reduces the computational complexity at the same time. The reason behind using CS encryption is that it provides unique output with less loss of information. The rest of paper is organized as follows: in Section 2, technical background of CS theory and FDCuT is given. In Section 3, information on the implementation of proposed technique is given. The results and discussion of proposed technique is given in Section 4. Finally, the conclusion is given in Section 5.

---

## Section snippets

### Preliminaries

In this section, technical information regarding Fast Discrete Curvelet Transform (FDCuT) and Compressive Sensing (CS) theory based encryption process are given. ...

### Proposed image hiding technique

In this section, the steps used for hiding a color secret image in host color medical image are presented. The CS based encryption is applied on the color secret image which is to be hidden into the host color medical image. The host color medical image and color secret image are first partitioned into R, G, and B channels, followed by four stages: Secret Image Encryption, Image Hiding, Extraction of Secret Image, and Decryption of Secret Image. Fig. 3 presents the concept of proposed image ...

### Results and discussion

The performance of the proposed image hiding technique is verified by different color medical images such as Knee MRI,<sup>1</sup> Brain MRI,<sup>2</sup> Lungs MRI,<sup>3</sup> Body CT,<sup>4</sup> and Liver US.<sup>5</sup> The image hiding in these color images is performed using color secret logo ...

### Conclusions

In this paper, an image hiding technique based on CS based encryption and Fast Discrete Curvelet Transform (FDCuT) is proposed for hiding color secret images in host color medical images. The combination of these two approaches proved to improve the authenticity to host color medical images and security to secret image at security point 1 and point 3 of standard teleradiology model. This proposed technique satisfies all requirements of color medical image security for telemedicine applications ...

## Declaration of competing interest

The authors declare no conflict of interest. ...

## Acknowledgments

This research work is funded by the Karnataka Science and Technology Promotion Society, Department of Information Technology, Bio Technology and Science & Technology, Government of Karnataka, India (No. KSTePS/VGST/SMYSR-2016-17/GRD-608/2017-18/90/366) under the category of Seed Money for Young Scientist Research (SMYSR), VGST Scheme. ...

[Special issue articles](#)   [Recommended articles](#)

---

## References (54)

H. Baur *et al.*

### [How to deal with security issues in teleradiology](#)

Computer Methods Programs Biomedicine (1997)

P. Ruotsalainen

### [Privacy and security in teleradiology](#)

European Journal of Radiology (2010)

R. Thabit *et al.*

### [A new robust lossless data hiding scheme and its application to color medical images](#)

Digital Signal Processing (2015)

ISO 27799:2016 (2016). Health Informatics – Information Security Management in Health using ISO/IEC 27002 (Online)....

Acharjee, S., Ray, R., Chakraborty, S., Nath, S., & Dey, N. (2014, July). Watermarking in motion vector for security...

Biswas, D., Das, P., Maji, P., Dey, N., & Chaudhuri, S.S. (2013, May). Visible watermarking within the region of...

Candes, E.J. (2006, August). Compressive sampling. In: Proceedings of the international congress of mathematicians...

E. Candes *et al.*

### Fast discrete curvelet transforms

Multiscale Modeling Simulation (2006)

E.J. Candes *et al.*

### New tight frames of curvelets and optimal representations of objects with piecewise C2 singularities

Communications Pure Applied Mathematics (2004)

E.J. Candes *et al.*

### An introduction to compressive sampling

IEEE Signal Processing Magazine (2008)



View more references

---

## Cited by (31)

### [A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications](#)

2022, Microprocessors and Microsystems

*Citation Excerpt :*

...Destructive attacks: This type of attack aims to erase the mark from the image. These approaches consider the mark as an additive noise and apply transformations to reduce or eliminate this noise [17]. Among the used methods are denoising, lossy compression, and quantization....

[Show abstract](#) ✓

### [DCT & DWT based watermarking scheme for medical information security](#)

2021, Biomedical Signal Processing and Control

*Citation Excerpt :*

...This message can be used to verify the integrity of the image, its authenticity, or for traceability purposes [7]. The three properties to be considered in a watermarking process are the capability that represents the amount of hidden information, the robustness that ensures that the hidden information is always accessible after modification of the watermarked image [8], and the imperceptibility that measures the degradation of an image by the integration process. Medical imaging is highly sensitive to noise [9], several sources can contribute to the generation of noise, e.g. the physical properties of sensors, the composition of the anatomical regions imaged and their structures [10]....

[Show abstract](#) ✓



# A modified salp swarm algorithm (SSA) combined with a chaotic coupled map lattices (CML) approach for the secured encryption and compression of medical images during data transmission

2021, Biomedical Signal Processing and Control

*Citation Excerpt :*

...Fig. 7 depicts the comparison of MS-SSIM with existing methods. Here, the results displays the proposed model achieves 90 %, the existing methods such as Arunkumar et al. [38] achieves 65 %, Borra et al. [25] achieves 72 %, Khedr [28] achieves the MS-SSIM value of 48 %, Raja [29] achieves the value of 55 %. Fig. 8 portrays the compression performance....

[Show abstract](#) ✓

## Medical Image Watermarking for Telemedicine Application Security ↗

2022, Journal of Circuits, Systems and Computers

## Watermarking techniques for medical data authentication: a survey ↗

2021, Multimedia Tools and Applications

## Secure image steganography using framelet transform and bidiagonal SVD ↗

2020, Multimedia Tools and Applications

[View all citing articles on Scopus](#) ↗

---

Conflict of Interest: No author associated with this paper has disclosed any potential or pertinent conflicts which may be perceived to have impending conflict with this work. For full disclosure statements refer to <https://doi.org/10.1016/j.smhl.2018.02.001> ↗.

[View full text](#)

© 2018 Elsevier Inc. All rights reserved.

