SVD-based Robust Image Steganographic Scheme using RIWT and DCT for Secure Transmission of Medical Images

S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, Naveen Chilamkurti, R. Logesh

PII: S0263-2241(19)30186-1
DOI: https://doi.org/10.1016/j.measurement.2019.02.069
Reference: MEASUR 6413

To appear in: *Measurement*

Received Date: 27 October 2018
Revised Date: 3 January 2019
Accepted Date: 25 February 2019

Please cite this article as: S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti, R. Logesh, SVD-based Robust Image Steganographic Scheme using RIWT and DCT for Secure Transmission of Medical Images, *Measurement* (2019), doi: https://doi.org/10.1016/j.measurement.2019.02.069

SVD-based Robust Image Steganographic Scheme using RIWT and DCT for Secure Transmission of Medical Images

Arunkumar S, School of Computing, SASTRA Deemed University, Thanjavur, India, **vgsarun@gmail.com**
Subramaniyaswamy V*, School of Computing, SASTRA Deemed University, Thanjavur, India, **vsubramaniyaswamy@gmail.com**
Vijayakumar V, School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, India, **vijayakumar.v@vit.ac.in**
Naveen Chilamkurti, Department of Computer Science and Computer Engineering, LaTrobe University, Melbourne, Australia, **n.chilamkurti@latrobe.edu.au**
Logesh R, School of Computing, SASTRA Deemed University, Thanjavur, India, **LogeshPhD@gmail.com**
***Correspondence: vsubramanyaswamy@gmail.com**

Abstract: The advances in computer technologies and the Internet have made rapid strides and breakthroughs in the field of data communication, which nowadays, is easily accessed. Unfortunately, this easy access offers almost endless opportunities for pirating copyrighted and confidential medical imagery. Many methods are proposed in the literature, however, most of them lack in robustness and perceptibility, and are prone to attacks. Hence, this study proposes a robust image steganographic approach that combines Redundant Integer Wavelet Transform (RIWT), Discrete Wavelet Transforms (DCT) and Singular Value Decomposition (SVD) and the logistic chaotic map. RIWT being a shift invariant, reversibility and robustness were achieved in this proposed technique. Better level of imperceptibility was achieved using SVD and DCT, with embedding carried out on singular values. Extra security was provided using the logistic chaotic map for encryption of secret medical images, which also enhanced the robustness of the technique. The effectiveness of our proposed scheme was compared with similar schemes available in the literature using common parameters such as imperceptibility, robustness and resistance to several geometric transformation attacks. This technique proved superior to other existing methods. The UCID benchmarking database was used during validation.

Keywords: Image Steganography; Logistic Chaotic Map; Singular Value Decomposition; Discrete cosine transform; Redundant Integer Wavelet Transform; Medical Image

1. Introduction

The strides made in computer techniques and the Internet have been rapidly increasing with countless breakthroughs occurring in the realm of data communication, which, in the present times, is readily accessible. The downside, however, is that this easy access provides limitless opportunities for stealing copyrighted and confidential imagers, especially those of the medical field. Therefore, the development of methods to secure such sensitive information is of great importance today.

The development of digital industries and the internet continues to accelerate. Usage is increasing globally. Because of increases in internet usage, the need to send confidential data has become imminent [1]. As multimedia technology grows at a rapid pace, so to do the tools and methods used to attack data transmitted over networks. For this reason, the risk associated with sending confidential data over the internet and the number of network based attacks have increased [2]. In response, confidential data or confidential images are seldom sent in plain, but instead in cipher form to the destination [3].

The literature presents two ways strategies for safeguarding data in transit: Cryptography and Information Hiding [4]. Cryptography is the transformation of secret data in plain text into a meaningless form called a cipher text using a secret key and cryptographic algorithm. The same key is required to decrypt a cipher text,and without knowledge of key, decryption is impossible [5]. Cryptography provides security to secret data, but because the cipher text is meaningless, this are always prone of suspicion present [6]. Some methodology is required to address both problems: providing security and evading suspicion. Information hiding solves both issues [7]. Security is provided because secret information is hidden within a cover medium. And, because the existence of secret information is not evident, suspicion is also averted. For transmitting secret images, information hiding is preferred to cryptography [8]. There are two types of Information Hiding: Steganography and water marking. Steganography is the process of concealing a secret within some other medium: text, image, video or even audio. This form of transmission is used for covert communication. Water marking's embedding method is similar to steganography, but its purpose is instead to provide authentication and restrict an image's unauthorized use [9].To carry the pay load of an image, the cover can also be an image. This process is called Image Steganography. Our proposed method employs an image as cover [10].

Steganographic techniques are divided into the following domains, spatial domain, transform domain, model based and spread spectrum. In spatial domain, secret information is hidden directly within a cover image. LSB embedding is a commonly used for the spatial domain. Human visual system may not be able to identify the existence of secrets in the cover medium, so spatial domain steganography provides stronger imperceptibility [11]. In transform domain, a cover image is subjected to any available transformation techniques, such as DCT, DFT, DWT, etc. A given cover image is split to obtain LL, LH, HL and HH sub-bands. The secret image is concealed in any of these sub-bands [12]. In spread spectrum, the secret image is concealed by modifying cover image noises introduced when the image is captured [13, 14]. In model based, a cover image is split into two parts. Embedding is not performed on the first part of an image, but embedding is performed in the second part –not by directly hiding the secret image in a portion of the cover image, but by exploiting cover image statistical characteristics [15]. Every domain has its own merits and demerits and is used for a specific purpose. For our purposes, the transform domain has been selected. In our present work, because we hope to provide a secure and robust system, the transform domain is most suitable.

1.1. SVD approaches to medical image security and their limitations

In a study [16] suggested a wavelet transform and block SVD-based blind watermarking method for the medical image security. In their method, confidential logo and electronic patient record information were embedded in singular values of sub-bands wavelets of the host images. The method was only limited to medical images. An approach that combined neural network, WT, and Rivest–Shamir–Adleman (R-S-A) encryption was proposed by Nagpal et al. [17] for protecting medical images. Kishore et al. [18] compared different approaches based on DWT-SVD, RSA-Discrete Wavelet Transform (DWT), and DWT-ANN. They observed that the DWT-SVD-based technique gave better results than the other methods. Hybrid techniques for protecting medical images were suggested by Singh et al. [19]. These methods combined SVD, DWT, spread spectrum, with crypto graphical ideas to secure medical images. In these methods, three different fault correction codes (Bose–Chaudhuri– Hocquenghem, Hamming, and Reed-Solomon codes) were utilized for encoding the secret medical images. These encoded images were embedded into coefficients of wavelets of the secret images into unique values of the image in an SVD type approach. It was concluded that the Reed–Solomon encoding of secret medical images presented better results than the others. Another method proposed [20] used an SVD-based method along with2D lifting wavelet transform (LWT) for protecting medical images. All these methods, while having similar embedding capacities, are vulnerable to attacks or present images of reduced quality. To deal with these limitations, this study proposes a novel hybrid steganographic technique which uses RIWT for better reversibility, SVD with DWT for enhanced robustness, and the logistic chaotic map for enhanced security.

1.2. Salient features of present approach

The proposed robust steganographic scheme is an advanced variant of approaches available in literature and is an improvement on existing methods due to following reasons:

1. Better security: The secret medical image is converted to a cipher image using Logistic Chaotic Map before it is concealed within cover image. This increases the security of the embedding process, makes the secret medical image unintelligible, and makes the stego image stronger against steganalysis.
2. Better robustness: RIWT, DCT use considerably increases the embedding rate and robustness level while enhancing the embedded secret's invisibility.
3. Lesser perturbation: Embedding is performed on singular values, which produces less perturbation in the cover image.

The cover image is first decomposed into 8×8 pixel sized non-overlapping blocks. Then, each block is separately subjected to RIWT transform. The secret medical image is encrypted using logistic chaotic map and then decomposed into 4×4 pixel sized non-overlapping blocks. The encrypted secret medical image is hidden in the transformed cover image. The SV of the cover image is modified to embed the SV of the secret medical image, because modification performed on singular values has a lesser overall effect on the cover image.

The remainder of the article is structured as follows: Section 2 lists similar contributions available in the literature, Section 3 describes preliminaries in our proposed work, Section 4 details our proposed

work, Section 5 furnishes the results of our proposed work and compares our findings with similar schemes, and Section 6 concludes and considers ideas for future study.

2. Literature Survey

In initial period of steganography, embedding is conducted on the Least Significant Bit (LSB) of every pixel of the cover image. LSB is either substituted with some secret image bits or modified to accommodate some bits of the secret image. The produced stego image is of good quality, because the existence of the secret image within it is not immediately evident [21]. If embedding is conducted on all the LSBs of the cover image and the same number of secret binary digits are concealed in LSB, steganalysis becomes easier. To avoid this problem, embedding is conducted at random locations and a random number of secret image bits is concealed within the cover image [22]. The cover image size determines the embedding capacity. A cover image is chosen based on the secret image's size. Embedding can be done on batch of cover images if the size of the secret image is too large to be embedded within a single cover image [23].

Numerous transform domain based steganography schemes are available within the literature. They use DCT, DFT, FFT, etc. Nowadays, wavelet based transform is more popular due to its multi resolution properties [24]. Some embedding schemes presented in the literature employ two or more transformation techniques. Experimental results prove the supremacy of this hybrid approach over approaches that use just a single transformation technique [25]. When the cover image is subjected to DWT transform, it is divided into LL, LH, HL and HH sub-bands. The LL sub-band contains a low frequency coefficient that represents the image's coarse information, while LH, HL and HH represent edge information [26]. Embedding in each sub-band produces a specific behavior. Embedding in the HH sub-band provides better imperceptibility but low robustness, while embedding in the LL sub-band provides better robustness but low imperceptibility [27].

DWT converts the cover image pixel value in integer value from the spatial domain to a floating point value to be used as the coefficient in the transform domain during the forward transform. In the inverse DWT transform, these floating point values of coefficients are converted into pixel integer values. Inverse transformation may not be accurate, so a DWT based algorithm may not provide accurate reversibility. To make an embedding algorithm reversible, IWT based embedding scheme is employed, but this method provides less robustness and capacity [28]. The Redundancy Discrete Wavelet Transform (RDWT) is a type of continuous wavelet transform approximation that differs from an orthogonal wavelet transform. An RDWT based embedding scheme provides better embedding capacity and greater robustness than a DWT based embedding scheme. [29]. To exploit the merits of better reversibility in IWT and better embedding capacity and strong robustness in RDWT, we propose a new algorithm: the Redundant Integer Wavelet Transform (RIWT). This algorithm provides accurate reversibility, better embedding capacity and strong robustness [30].

Both cover and secret images are subjected to DCT transform to obtain a coefficient. The transformed coefficient of the secret image is concealed in the transformed cover image coefficient. The obtained stego image is proven to be more robust and able to withstand different steganalysis attacks [31]. Patient information is represented in a secret image that must be concealed within a cover image. The chosen cover image is also a medical image. DCT and DWT are applied to the images before embedding. Performance is evaluated to be better resisting many kinds of attacks [32].

Many matrix factorizing techniques are available, namely Singular Value Decomposition (SVD), QR Decomposition, LU Decomposition, etc. Among these, SVD is widely used in image steganography because it provides better invisibility [33]. SVD is a reliable and stable orthogonal decomposition method that splits a given image into three constituent matrices, U, S and V. S is diagonal non-negative Singular Values (SV). Small changes in SVs do not disturb overall image quality [34].

Various healthcare applications based on wireless medical sensor network (WMSN) have been surveyed for IoT environment. Security techniques that are used for handling the healthcare systems security issues, especially for hybrid security techniques have also been discussed [35, 42]. A method to study the medical image quality degradation when hiding data in the frequency domain is proposed. In the embedding process, the secret plaintext was converted into cipher usingRC4 encryption and cover image was transformed using Discrete Fourier Transform (DFT). The results prove that produced stego image is of low quality if embedding is done in low frequency sub-band, where as quality degradation of stego image is less if embedding is done in high frequency [36].

3. Preliminaries

The following section briefly explains the methods used by our proposed method.

3.1. Redundancy Integer Wavelet Transform (RIWT)

DWT uses floating point coefficients in both the image's forward and inverse transformations. Image pixel values are always integer values. Due to the conversion of integer pixel values into floating point coefficients, some errors in the forward and inverse transformations are introduced. IWT avoids floating point coefficients and uses integer coefficients. Integer pixel values are mapped to integer coefficient value using a Haar lifting transform, a popular retrievable transform. The following equations are used for forward and inverse transforms:

$$d_{1,x} = S_{0,2x+1} - S_{0,2x} \quad (1)$$

$$s_{1,x} = s_{0,2x} + \lfloor d_{1,x/2} \rfloor \quad (2)$$

$$S_{0,2x+1} = d_{1,x} + s_{0,2x} \quad (3)$$

$$S_{0,2x} = s_{1,x} - \lfloor d_{1,x/2} \rfloor \quad (4)$$

RDWT may be considered an approximation of a continuous wavelet transform, which is a non-orthogonal wavelet transform type. RDWT provides more embedding capacity and is stronger and more robust than DWT. A single image is decomposed using RDWT.A one-dimensional transform is conducted on an image using low-pass and high-pass filters. Rows are transformed into low frequency and high frequency coefficients, and columns are subjected to a one-dimensional RDWT transform. Finally, a single image is decomposed into four coefficient matrix: D,H,V and A. Decomposition is performed repeatedly until a satisfactory decomposition level is obtained. Because a constant sampling rate is maintained by RDWT, translation is space invariant. This transform has the property of time-shift invariance and introduces redundancy.

To capitalize on the advantages of IWT and RDWT, a new algorithm, RIWT, is constructed by combining these two transforms. RIWT provides strong reversibility and high invisibility properties than DWT and IWT. For these reasons, RIWT is utilized in our proposed scheme.

3.2. Image Encryption using Logistic Chaotic Map

The image is encrypted to modify pixel values, which renders the input image unintelligible to confuse the third party and make information transmission safer. Moreover, image encryption is found to improve the robustness of embedding schemes.

Chaotic map provides chaotic sequences with numbers in an unpredictable manner. It is defined by the following polynomial equation:

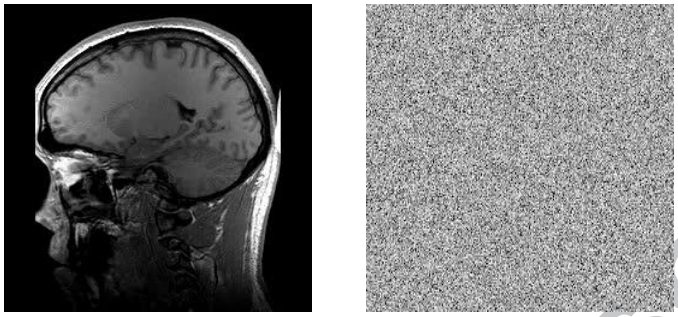
$$L_{n+1} = \mu L_n (1 - L_n) \quad (5)$$

Where L_n represents population at any given generation n, and the parameter μ denotes growth rate with a value in the range [0,4]. The chaotic map generated with an initial value $L0 \in (0,1)$ and $\mu \in [3.5699456, 4]$ is neither periodic nor convergent and is largely chaotic in nature. Because of this property, a logistic chaotic map is used in our proposed scheme.

Image Encryption and decryption are identified as defined in (6):

$S_{en} = S \oplus CS$ and $S = S_{en} \oplus CS$ (6)

Where S_{en}, S denotes an encrypted secret image and decrypted secret image, $\oplus$ denotes XOR operation and CS denotes chaotic sequence. The values of parameter L_0 and μ in (5) are treated as secret keys. The secret plain image and its cipher image are shown in Fig.1. Cipher secret image provides the best uncorrelated and non-periodic properties.



(a) Test secret image (b) cipher image

Fig.1: (a) Test secret and (b) cipher images. The cipher secret image offers superior uncorrelated and non-periodic properties

3.3. SVD

SVD is a reliable and stable decomposition scheme for an orthogonal matrix. It divides the given matrix optimally so that every linear independent set exists with its original contribution of energy. The N x N sized digital image A can be split by SVD as shown below,

$$\text{SVD (A)} = \begin{pmatrix} L1\ L12 \dots L1n \\ L21\ L22 \dots L2n \\ . \\ . \\ . \\ Ln1\ Ln2 \dots Lnn \end{pmatrix} \begin{pmatrix} \sigma 11\ 0 \dots 0 \\ 0\ \sigma 22 \dots 0 \\ . \\ . \\ . \\ 0\ 0 \dots \sigma nn \end{pmatrix} \begin{pmatrix} R11\ R12 \dots R1n \\ R21\ R22 \dots R2n \\ . \\ . \\ . \\ Rn1\ Rn2 \dots Rnn \end{pmatrix}^{T} \quad (7)$$

Where

- L denotes a left unitary matrix of size n x n with orthogonal columns, i.e., L^T x L = IM_n, where IM_n is the identity matrix.
- R denotes a right unitary matrix and is also an orthogonal matrix $R^T = R^{-1}$.
- σdenotes a non-negative rectangular diagonal matrix of size n x n, these values are Singular Values (SV), which are in a sorted order or satisfy$\sigma 11 > \sigma 22 > \sigma 33 \dots \sigma nn$.

Small modifications done on SV do not affect the overall perceptual quality of an image. Even with multiplication operations, other image processing operations, like transpose, flipping, and rotation, are done on SV, so its original meaning is not changed. Due to this attractive property, SVD is widely used in image processing applications.

3.4. DCT Transform

Forward 2D Discrete Cosine Transform is defined by,

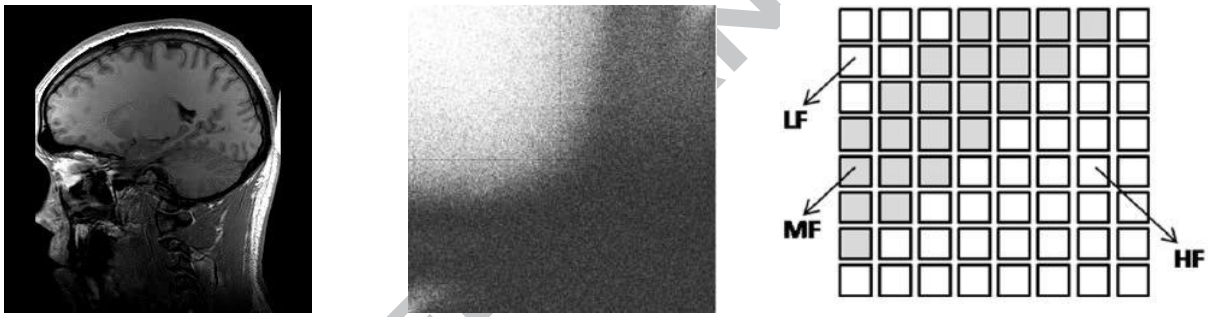
$$F(a,b) = \sigma(a)\sigma(b) \sum_{l=0}^{N-1} \sum_{m=0}^{n-1} f(l,m) \cos\left[\frac{(2l+1)\pi}{2N} a\right] \cos\left[\frac{(2m+1)\pi}{2N} b\right] \quad (8)$$

Where a,b =0,1,…N-1. 2D DCT transformation has symmetric properties as well as an orthogonal property. σ(a), σ(b) and the inverse 2D DCT can be expressed by (9) and (10)

$$\sigma(a) = \begin{cases} \frac{1}{\sqrt{N}} & a = 0 \\ \frac{2}{\sqrt{N}} & a \neq 0 \end{cases} \sigma(b) = \begin{cases} \frac{1}{\sqrt{N}} & b = 0 \\ \frac{2}{\sqrt{N}} & b \neq 0 \end{cases} \quad (9)$$

$$f(l,l) = \sum_{l=0}^{N-1} \sum_{m=0}^{n-1} \sigma(a)\, \sigma(b) F(a,b) \cos\left[\frac{(2l+1)\pi}{2N} a\right] \cos\left[\frac{(2m+1)\pi}{2N} b\right] \quad (10)$$

DCT is good for providing energy compaction and is used for compressing imagesas well as for signal processing applications. DCT segments images into low frequency (LF) sub-bands, medium frequency (MF) sub-bands and high frequency (HF) sub-bands according to secret image quality, as shown in Fig.2 (a).Fig.2 (b) shows the transform coefficient and (c) distribution of coefficients, which goes from the top right to the bottom left of an image. It is inferred that low frequency components (brighter regions) are large in magnitude. If embedding is completed in this region, image quality changes drastically, so this region is not preferred for embedding. High frequency components (darker regions) are smaller in magnitude and carry some image information. Through compression or some image processing attacks, this region may be eliminated easily, so this region is also omitted in the embedding process. Secret images are concealed in the medium frequency sub-bands.



(a) (b) (c)

Fig.2: (a) secret image (b) transform coefficient showing the dark and light regions (c) Frequency bands of coefficients showing low, mid and high frequencies with directions

4. Proposed Methodologies

A new secure and robust steganographic scheme is proposed in this section. The secret medical image is encrypted using a logistic chaotic map to obtain a cipher image and cover image in spatial domain is converted into the coefficient matrix of the frequency domain using RIWT. DCT is applied to both the cipher images and the coefficient matrix, and then SVD is applied to obtain singular values for both. DCT transformed cipher images are concealed in a DCT transformed coefficient matrix of cover images. The proposed methodology is divided into an embedding phase and extraction phase, which are explained in section 4.1 and 4.2, respectively.

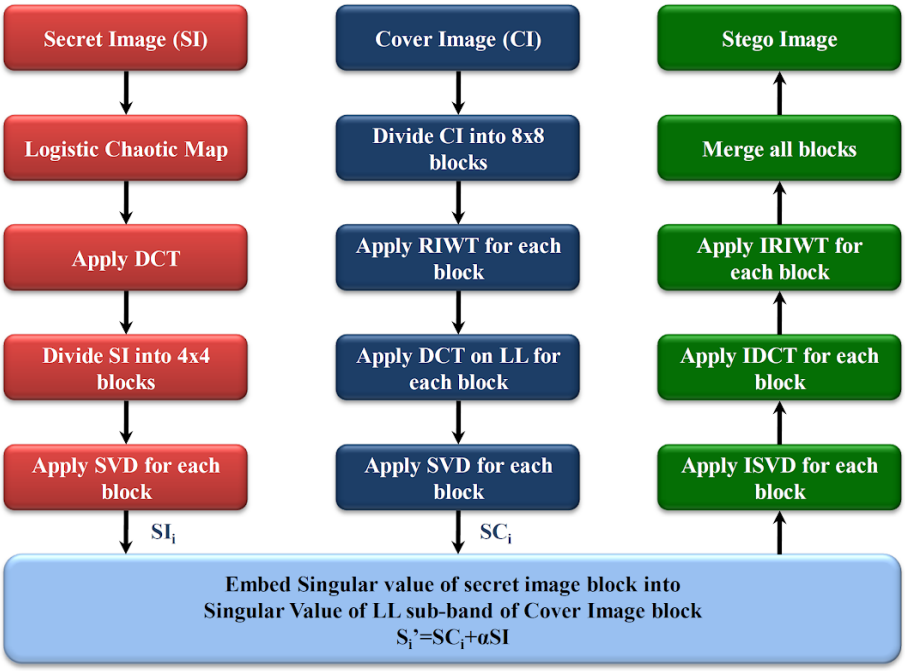


Fig.3 Embedding process of secret image block into cover image block

4.1. Embedding Phase

Cover image C of size 512 x 512 pixels is decomposed into blocks of 8 x 8 pixels and each block is subjected to RIWT transformation. The LL sub-band is subjected to 2D DCT transform to obtain coefficient. Secret medical image I of size 256 x 256 pixels is encrypted using an image encryption algorithm by Logistic Chaotic Map, and is subjected to 2D DCT transform to obtain coefficient and is decomposed into blocks of 4 x 4 pixels. SVD is applied both to the coefficient of the secret medical image and the cover image. The SV of secret medical image I is embedded into cover image C. Fig.3 shows the embedding phase and is explained as below,

Input: Cover image C with a size of 512 x 512, Secret image I with a size of 256 x 256

Output: Stego image S with a size of 512 x 512.

Step 1: Cover image C is decomposed into non-overlapping blocks of size 8 x 8 pixels. CB_i represents the i^{th} cover image block.

Step 2: Secret image I is encrypted using the Image Encryption algorithm by Logistic Chaotic Map.

Step 3: Encrypted secret image I is subjected to 2D DCT transform to produce coefficient matrix J.

Step 4: J is decomposed into blocks of 4 x 4 pixels. JB_i represents the i^{th} secret image block.

Step 5: SVD is applied to each JB_i block as follows to decompose a single matrix into three constituent matrices,

SVD (JB_i) = UI_i x SI_i x VI_iWhere SI_i represents Singular values of JB_i.

Step 6: Following steps are performed for each block of CB_i

1. CB_i is transformed using 1-level RIWT to produce four sub-bands, LL, LH, HL and HH. Embedding is completed in the desired sub-band, preferably in LL.

2. The LL sub-band of CB_i is subjected to 2D DCT transform to produce coefficient matrix D_i.

3. SVD is applied to coefficient matrix D_i of each block of cover images as follows to decompose a single matrix into three constituent matrices,

$$SVD\ (D_i) = UC_i \times SC_i \times VC_i$$

Where SC_i is singular values of sub-band of CB_i block.

4. SV of SI_i is embedded into SV of SC_i of C_i as follows,

$$S'_i = SC_i + \alpha \times SI_i$$

Where α is the scaling factor, which is utilized to strengthen the embedding.

5. The inverse of SVD is performed as follows,

$$\text{Inverse of SVD (sub-band of } CB_i) = UC_i \times S'_i \times VC_i$$

6. The value obtained is subjected to the inverse of 2D DCT transform to obtain a modified LL sub-band.

7. The inverse of RIWT is obtained using modified LL with other three sub-bands to produce a stego image block SB_i.

Step 6: All stego image blocks SB_i are concatenated to produce Stego image S.

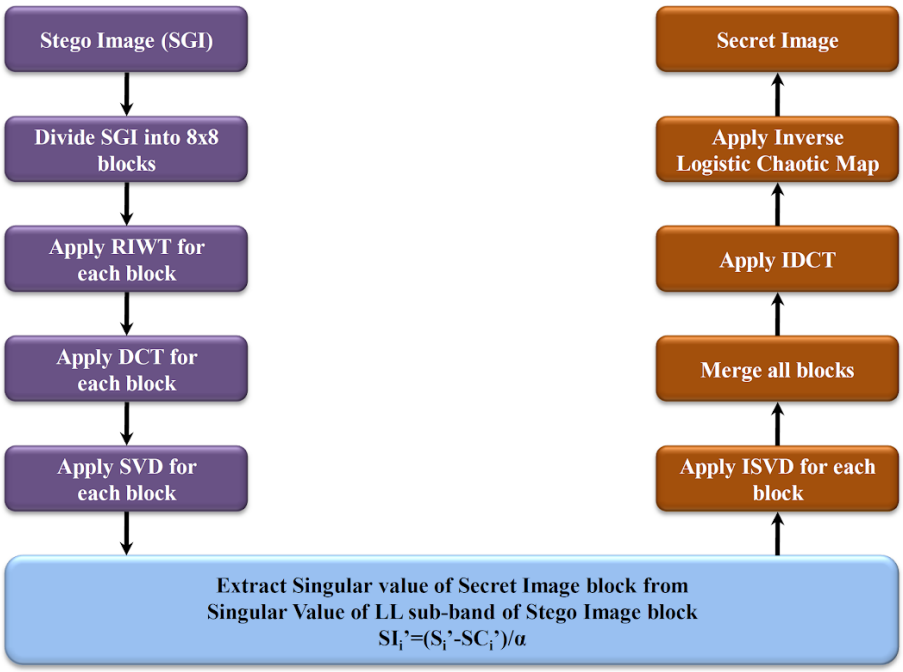


Fig.4: Extraction process of secret image from stego image block

4.2. Extraction Phase

Stego image S of size 512 x 512 is decomposed into blocks of 8 x 8 pixels and each block is subjected to RIWT transformation and then to 2D DCT transform. SVD decomposition is performed on the sub-band LL to obtain the Singular value S_i. The S_i calculated in this phase and in the embedding phase is used to obtain encrypted secret medical image block I_i. Then, all I_i blocks are merged to construct

Secret medical image I' with size 256 x 256. I' is subjected to a reverse Logistic Chaotic Map to produce secret medical image I. The extraction phase, as shown in Fig.4, is explained as below,

Input: Stego image S of size 512 x 512, and three values obtained in embedding phase namely SC_i, UI_i and VI_i.
Output: Secret medical image I of size 256 x 256.

Step 1: Stego image S is divided into non-overlapping blocks of size 8 x 8 pixels. SB_i represents the i^{th} stego image block.

Step 2: Following steps are performed for each Stego image block SB_i

1. SB_i is transformed using 1-level RIWT to produce four sub-bands LL, LH, HL and HH.
2. LL sub-band of SB_i is subjected to 2D DCT transform.
3. SVD is applied to LL sub-band of SB_i as follows,

   SVD (sub-band of SB_i) = U_i x S'_i x V_i

   Where S'_i are Singular values of the sub-band of SB_i block.
4. Secret image block JB_i is extracted as follows,

   $Di = (S'_i - SCi) / \alpha$
5. The inverse of SVD is applied to obtain JB_i.

   $JBi = UI_i$ x Di x VI_i

   where UI_i and VI_i are received from the embedding phase.

Step 3: All JBi blocks are merged to construct J.

Step 4: J is subjected to the inverse of 2D DCT transform.

Step 5: J is Decrypted using the Image Decryption algorithm by the Logistic Chaotic Map to obtain secret image I.

5. Experimental Results and Analysis

We have performed simulation using MATLAB R2017b. Different experiments are conducted to evaluate our scheme using common parameters like imperceptibility, resistance to steganalysis, and robustness, which are discussed in section 5.2, 5.3, and 5.4, respectively. To evaluate our proposed scheme, similar schemes are taken as baseline schemes for comparison, as discussed in section 5.5. Many secret images were tested with our proposed methods for more number of cover images. As embedding provides almost similar effects, Evaluation of our scheme is demonstrated with a secret image of size 256 x 256 and 8 cover images of size 512 x 512 as shown in Fig.5 and Fig.6.

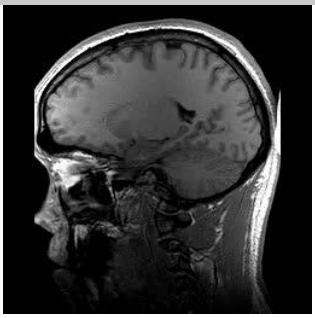


Fig. 5: Secret image

(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 6 : Selected cover images of size 512×512

5.1. Performance evaluation metrics

For the purpose evaluating the performance of our proposed scheme, various metrics, like peak signal to noise ratio (PSNR), image fidelity (IF) , normalized absolute error (NAE), normalized cross correlation (NCC) and mean structural similarity index (MSSIM) are used.

PSNR is a parameter widely used to assess the produced stego image quality. It is computed as shown below,

$$\text{PSNR} = 10 \log_{10}\left(\frac{255^2}{MSE}\right) \quad (11)$$

Where MSE is the mean squared error between cover and stego image, which is determined by,

$$MSE = \sqrt{\frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(C(a,b)-(C'(a,b))^2}{mXn}} \quad (12)$$

Where m and n are the number of rows and columns, C(a, b) is cover image and C'(a, b) is stego image. High stego image indicates good quality.

The MSSIM metric is also used to assess image quality. Using this metric, the luminance, contrast and structure of two images are compared. It is calculated for many windows of an image. The difference between N X M sized windows, x and y, is measured by,

$$MSSIM\ (X,Y\ ) = \frac{1}{M}\sum_{j=1}^{M} \mathrm{SSIM}(x_j, y_j) \quad (13)$$

Where X denotes cover image, Y denotes stego image, and x_j and y_j are the contents of image at the j^{th} local window, M is the number of windows. SSIM is measured by,

$$SSIM\ (X,Y) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)} \quad (14)$$

Where μ_x and μ_y are the mean of x, y respectively, σ_x^2 and σ_y^2 are the variances of x, y respectively, σ_{xy} is the co-variance of x and y. C_1 and C_2 are variables to stabilize the division with weak denominators. The MSSIM value needs to be close to 1.

Normalized Absolute Error is calculated by,

$$NAE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(C_{i,j} - C\prime_{i,j})}{\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{i,j})} \quad (15)$$

Image Fidelity is calculated by,

$$IF = 1 - \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(C_{i,j} - C\prime_{i,j})^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{i,j})^2} \quad (16)$$

Where $C_{i,j}$ and $C'_{i,j}$ are the image intensity at the location i, j of the original and extracted secret images, respectively. The NAE have be as close to zero and the IF value needs to close to 1.

Normalized cross correlation is computed by,

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[C_{i,j} - \mu_s][C'_{i,j} - \mu'_s]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[C_{i,j} - \mu_s)^2]}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(C'_{i,j} - \mu'_s)^2}} \quad (17)$$

Where $C_{i,j}$ and $C'_{i,j}$ are the intensities of the original and extracted secret images, respectively, at the i^{th} and j^{th} location, and μ_s and μ_s' are the means of the original and extracted secret images, respectively. NCC coefficients provide an amount of similarity between the original secret images and the extracted secret images and the range of their values have to be between -1 and 1. If two images are perfectly the same, then NCC is 1; if two images are uncorrelated, NCC is 0; otherwise, if two images are completely opposite, then NCC is -1.

5.2. Imperceptibility

Imperceptibility is the measure of the invisibility of presence of a secret image in the produced stego image. It is evaluated using PSNR, MSSIM, NAE, IF and NCC.

(a) (b) (c)

Fig.7. (a) Cipher image (b) Extracted image using correct key (c) Extracted image using wrong key.

The secret medical image shown in Fig 5 is embedded into all the cover images shown in Fig.6. Fig.7 shows the stego images produced by embedding secret medical images in all the cover images. Fig 7.(a) shows the encrypted secret medical image. This is done to provide more security. Even if the extraction algorithm is known, without the encryption key, extraction cannot be completed properly. Fig.7.(b) shows the deduced stego image through the proper key and Fig.7.(c) displays the extracted stego image through an improper key.

All the stego images shown in Fig.8 produce better PSNR values, with values ranging between 49.26 and 50.18. This is better than the similar scheme available in the literature, as shown in Table 2. MSSIM and all the stego image's NCC values are close to 1, which is the desirable value. The NAE value is close to zero, which is also the desirable value. So, from the above findings, we can infer that RIWT-DCT have improved our proposed scheme to produce stego images with better imperceptibility properties than DWT-DCT and IWT-DCT.

5.3. Resistance to steganalysis

Using steganalysis, hidden information can be deduced from stego images without using either the proper key or extraction algorithm. Due to advancements in the steganography algorithm, it is not easier to steganalyse a stego image without knowledge of the key or algorithm. An advanced steganographic algorithm minimizes the effect of changes that can be identified by the human eye. However, it changes the statistical behavior of an image, which can be identified through careful analysis. To assess the resistance strength of our proposed scheme against steganalysis, algorithms proposed in [37,38] are used. In wavelet based steganalysis (WBS), images are decomposed using quadrature mirror filters(QMF), which segments the frequency space of an images' transform domain into varying orientations and scales. To achieve this, separable low-pass and high-pass filters are applied along the image axis, producing vertical, horizontal, diagonal and low frequency sub-bands. The horizontal, vertical and diagonal sub-band's mean, variance, skewness and kurtosis are obtained in the first set of statistics. The coefficient magnitude's optimal linear predictor error is the basis for the second set of statistics. Support Vector Machine (SVM) is trained to calculate the above statistics. Using this, clean images and stego images are analyzed and differentiated.

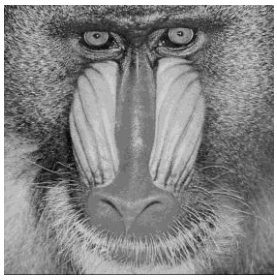
As a contourlet transform based approach provides enhanced directionality, the second approach for steganalysis is based on this transform. Contourlet coefficient moments are highly sensitive to embedding of secrets, as contourlet transform is more scattered when compared to wavelets. For the purpose of steganalysis, the given image is transformed in level 3, thus producing 8 different sub-bands. Variance, skewness, mean and kurtosis moments for all the sub-bands and the difference between the actual coefficient and the linear predicted coefficient results in a feature set with 64 dimensions. To discriminate cover image from stego image, a non-linear type of support vector machine is used.

PSNR= 49.33
MSSIM= 0.9893
NAE= 0.0014
IF= 1.0
NCC= 0.9963

PSNR= 49.27
MSSIM= 0.9928
NAE= 0.0021
IF= 0.9998
NCC= 0.9998

PSNR= 49.67
MSSIM= 0.9957
NAE= 0.0018
IF= 0.9997
NCC= 0.9997

PSNR= 50.02
MSSIM= 0.9892
NAE= 0.0019
IF= 0.9997
NCC= 0.9996



PSNR= 49.26
MSSIM= 0.9914
NAE= 0.0019
IF= 0.9997
NCC= 0.9997

PSNR= 50.12
MSSIM= 0.9958
NAE= 0.0020
IF= 1.0
NCC= 0.9999

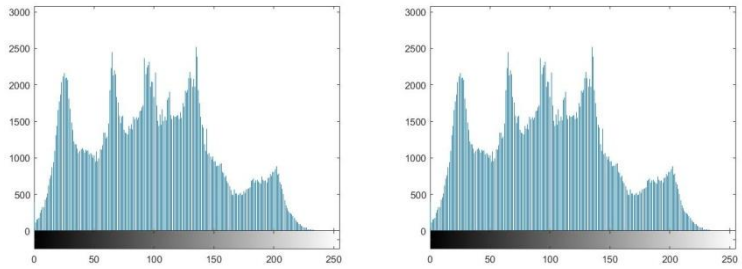
PSNR= 50.18
MSSIM= 0.9857
NAE= 0.0014
IF= 0.9999
NCC= 0.9996

PSNR= 49.96
MSSIM= 0.9942
NAE= 0.0016
IF= 0.9998
NCC= 0.9997

Fig. 8: Imperceptibility measure results of proposed scheme

To perform steganalysis, 500 cover images from the UCID database are used. Secret medical images presented in Fig.6 are embedded into all the cover images chosen using our proposed method. Statistics are collected from 500 cover images and their corresponding stego images. True positive (TP) refers to the correct identification of a stego image as a stego image or of a cover image as a cover image. False positive (FP) refers to incorrectly identified images. The average TP value for WBS is 53 % and for CBS is 58 %. The average TP value indicates the steganalyzer's poor ability to detect an image as stego or cover. The above experimental results indicate that the steganalyzer is unable to differentiate between cover image and stego image, and many times a cover image is wrongly classified as a stego image and a stego image is wrongly classified as a cover image. Based on the experimental results, proposed algorithm is undetectable and certified to be secure.

Histogram attack is also considered for the purpose of evaluation of security. If a histogram difference of the cover and its stego-image is observed, then the image is considered suspicious. Histogram of Lena cover image and its corresponding stego image produced by algorithm are shown in Fig.9. Fig.9(a) is histogram of cover image and 9(b) is histogram of its stego image. Both look alike, so steganalyser will not try to attack stego image. Based on the experimental results, proposed algorithm is undetectable through a histogram attack.



(a) (b)

Fig.9: Histogram of cover image and its stego image

5.4. Robustness

Robustness is the measure of the ability to extract the embedded secret image properly from the attacked stego image. It is measured using MSSIM, NCC and Bit error rate (BER). All three parameters gauge the similarity between the extracted secret image and the original secret image.

To evaluate the robustness of our proposed scheme, cover images Barbara, House, Pepper and Airplane, as shown in Fig.6, are considered. They are resized into 256 x 256 secret images and are embedded into Lena as cover images, which is also shown in Fig.6 to produce four different sets of stego images. To test the robustness of our proposed scheme, these four sets of stego images are subjected to some image processing attacks, as shown in Fig.10. In Fig.10 (a), the stego image is resized 1024 x 1024; in (b), it is rotated 15^0; in (c), it is subjected to image sharpening operating; in (d), it is subjected to blur operation; in (e), it is combined with gaussian noise with a variance of 0.001; in (f), it is combined with salt & pepper noise with density 0.001; in (g), it is combined with Speckle noise with variance 0.001; in (h), it is subjected to a Median filter with a filter size of 3 x 3; in (i), it is subjected to a Wiener filter with a filter size of 3 x 3; in (j), it is cropped; in (k), it is subjected to Shear; and finally in (l), it is subjected to JPEC compression with QF 75 %. The secret image is extracted properly from all attacked stego images. From this four set, MSSIM, BER and NCC are computed between the original secret and the extracted secret, as shown in Table 1. From this table, MSSIM and NCC values are close to 1 and BER is close to 0, which is the desirable result. So, it is inferred that our scheme is robust enough to resist image processing attacks.

Table 1 : Extracted secret image's value for the parameters MSSIM, BER, NCC from stego images that are attacked.

Attacks	**Barbara**			**House**			**Pepper**			**Airplane**		
	MSSIM	**NCC**	**BER**	**MSSIM**	**NCC**	**BER**	**MSSIM**	**NCC**	**0.0121**	**MSSIM**	**NCC**	**BER**
Resize [1024 1024]	0.7813	0.9832	0.0143	0.7467	0.9754	0.0124	0.8645	0.9784	0.0116	0.7465	0.9867	0.0165
JPEC compression with QF=75	0.7476	0.9562	0.0144	0.7173	0.9556	0.0134	0.8179	0.9847	0.0139	0.7410	0.9733	0.0185
Crop	0.6142	0.9327	0.0168	0.6784	0.9431	0.0161	0.7302	0.9587	0.132	0.6832	0.9243	0.0162
Shear	0.7545	0.9685	0.0148	0.6892	0.9511	0.0165	0.7782	0.9875	0.0196	0.7106	0.9612	0.0134
Rotate 15^0	0.7243	0.9432	0.0165	0.7047	0.9532	0.0147	0.7463	0.9624	0.0198	0.7216	0.9847	0.0154
Blur	0.8708	0.9975	0.0146	0.7693	0.9874	0.0138	0.8536	0.9938	0.0153	0.7385	0.9743	0.0129
Sharpen	0.6525	0.8759	0.0187	0.6285	0.8951	0.0196	0.6735	0.9179	0.0107	0.6708	0.8676	0.0199
Wiener filter [3 3]	0.7759	0.9728	0.0143	0.7582	0.9825	0.0127	0.8355	0.9912	0.0121	0.7611	0.9699	0.0128
Median filter [3 3]	0.7765	0.9781	0.0133	0.7653	0.9625	0.0205	0.8327	0.9869	0.0221	0.7457	0.9736	0.0136

Speckle noise with variance 0.001	0.7105	0.9463	0.0146	0.6590	0.9476	0.0156	0.7655	0.9884	0.0137	0.6929	0.9488	0.0162
Salt & pepper noise with density 0.001	0.6472	0.9018	0.0172	0.6217	0.8745	0.0173	0.6436	0.9182	0.0142	0.6106	0.8693	0.0174
Gaussian noise with variance 0.001	0.6831	0.9427	0.0168	0.6574	0.9381	0.0161	0.6877	0.9673	0.0183	0.6539	0.9638	0.0148

(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

Fig.10. Stego images under various attacks (a) Resize [1024 2014] (b) Rotate 15° (c) Sharpen (d) Blur (e) Gaussian noise with variance of 0.001 (f) Salt & pepper noise with variance of 0.001 (g) Speckle noise with density of 0.001 (h) Median filter with filter size [3 3] (i) Wiener filter with filter size [3 3] (j) Crop (k) Shear (l) JPEC compression with QF=75.

5.5. Comparison with similar schemes

In this section we show that our method is superior to similar methods available in the literature. For comparison, we have taken three schemes, Chang et al. [39], Wu et al. [40] and Kanan et al. [41], and we use three parameters, PSNR,NCC and MSSIM. Table 2 shows the comparison results of ours with the other schemes for the three parameters. Table 2 also shows the average value for PSNR, NCC and MSSIM for ours and the remaining three schemes. The average value for PSNR, NCC and MSSIM of Chang et al. [39] are 40.79, 0.9815, and 0.9877, respectively. The values for these three parameters are good, so scheme produces reasonably good quality stego images. The average values for PSNR, NCC and MSSIM of Wu et al. [40] are 40.18, 0.9895, and 0.9893, respectively. The average values for NCC and MSSIM are better that [39], indicating better quality stego images. Average value for PSNR, NCC and MSSIM of Kanan et al. [41] is 45.12, 0.9879 and 0.9907. The average values for NCC and MSSIM are better than [39] and [40], indicating that this scheme produces better quality stego images. The average values of PSNR, NCC, and MSSIM of our scheme are 49.77, 0.9997, and 0.9930, respectively. These values are better than [39], [40] and [41].

Table 2 : Comparison of ours with similar schemes

Algorithm	Cover image	PSNR	NCC	MSSIM
Chang et al[39]	Lena	40.37	0.9832	0.9901
	Airplane	43.54	0.9814	0.9875
	Pepper	39.30	0.9811	0.9886
	Baboon	39.94	0.9804	0.9846
	Average	**40.79**	**0.9815**	**0.9877**
Wu et al[40]	Lena	40.17	0.9913	0.9840
	Airplane	41.23	0.9921	0.9913
	Pepper	39.27	0.9858	0.9885
	Baboon	40.04	0.9889	0.9936
	Average	**40.18**	**0.9895**	**0.9893**
Kanan et al [41]	Lena	45.12	0.9845	0.9889
	Airplane	45.18	0.9862	0.9916
	Pepper	45.12	0.9885	0.9895
	Baboon	45.13	0.9925	0.9928
	Average	**45.13**	**0.9879**	**0.9907**
Proposed Method	Lena	50.12	0.9999	0.9958
	Airplane	50.02	0.9996	0.9892
	Pepper	49.67	0.9997	0.9914
	Baboon	49.26	0.9997	0.9957
	Average	**49.77**	**0.9997**	**0.9930**

Graphical comparison of Table 2 is shown in Fig. 11, Fig.12 and Fig.13. In Fig.11, the x-axis represents the four scheme and y-axis represents the PSNR values for each images against each image. For each scheme, four bars represent the values of each image. For all the images, the value of the proposed scheme is higher than the similar schemes. Similarly, in Fig.12 and Fig.13, the x-axis represents the four schemes and the y-axis represents theNCC and MSSIM values, respectively.In these two figure also, the value of the proposed scheme's bar is greater than the other three schemes. This indicates that our scheme is superior to similar schemes available in the literature.

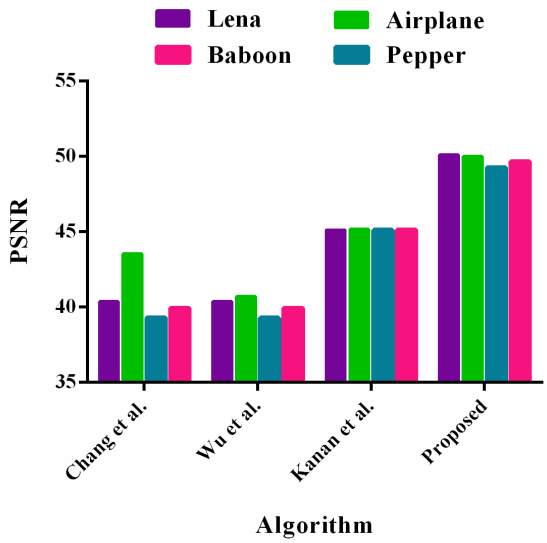


Fig.11 : Comparison of PSNR value of proposed method with similar schemes

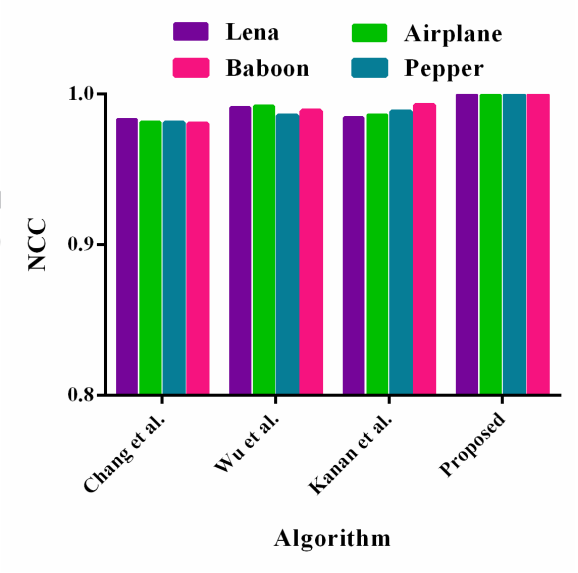


Fig.12 : Comparison of NCC value of proposed method with similar schemes

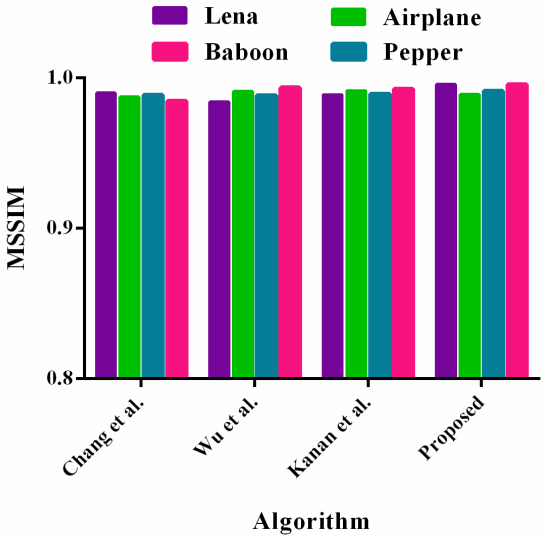


Fig.13: Comparison of MSSIM value of proposed method with similar schemes

6. Conclusion and Future Enhancement

A robust image steganographic scheme based on RIWT, DCT and SVD has been proposed in our paper. This scheme has combined the technology of RIWT, DCT, the SVD decomposition technique and the logistic chaotic map. As RIWT is a shift invariant, reversibility and robustness are achieved in our proposed scheme. Better imperceptibility is achieved by using SVD and DCT, as embedding is completed on singular values. Usage of the logistic chaotic map to encrypt secret medical images provides extra security and also improved robustness to our scheme. As decomposition is done using SVD and embedding is done on a specific sub-band of decomposed block, steganalysis has become a tough task. Moreover, modification of the SVs of SVD efficiently resists geometric attacks and attacks by image manipulation. The experimental results, as well as the analysis and comparison with similar schemes in the literature, show that our scheme is superior to other schemes in terms of imperceptibility, reversibility and robustness. Confidentiality is a key requirement in healthcare areas such as Telemedicine. The medical image needs to be secured during transmission. Authentic images and their integrity are prime requirements in healthcare. This proposed method can provide authenticity and integrity of the medical images in the transmission process, and cryptography can ensure the confidentiality of these medical images. The method can be used for Military applications too, where secrecy is a must. In the future, we plan to enhance the steganography framework by embedding secret medical image blocks only in few cover image blocks based on statistical measure like contrast and correlation.

References

[1] A Cheddad, J Condell, K Curran, PM Kevitt , Digital image steganography: Survey and analysis of current methods, Signal Process 90(3) (2010)727–752

[2] MS Subhedar, VH Mankar, Image steganography using redundant discrete wavelet transform and QR factorization, Computers & Electrical Engineering. 1(54) (2016)406-22.

[3] A Miri, K Faez, An image steganography method based on integer wavelet transform, Multimedia Tools and Applications. 77(11) (2018)13133-44.

[4] A Anees, AM Siddiqui, J Ahmed, I Hussain, A technique for digital steganography using chaotic maps, Nonlinear Dynamics. 75(4) (2014)807-16.

[5] B Liu, RR Martin, JW Huang, SM Hu, Structure aware visual cryptography In Computer Graphics Forum. 33(7)(2014) 141-150

[6] KH Lee, PL Chiu, Image size invariant visual cryptography for general access structures subject to display quality constraints, IEEE transactions on image processing. 22(10) (2013)3830-41.

[7] S Nazari, AM Eftekhari-Moghadam, and M Shahram Moin, A novel image steganography scheme based on morphological associative memory and permutation schema, Security and Communication Networks. 8(2)(2015) 110-121.

[8] V Thanikaiselvan, P Arulmozhivarman, RAND-STEG: an integer wavelet transform domain digital image random steganography using knight's tour, Security and Communication Networks. 8(13)(2015)2374-82.

[9] JC Judge, Steganography: past, present, future. Lawrence Livermore National Lab., CA (US) 200.

[10] N Provos, P Honeyman, Hide and seek: An introduction to steganography. IEEE security & privacy. 99(3) (2003)32-44.

[11] KH Jung, KY Yoo, Steganographic method based on interpolation and LSB substitution of digital images, Multimedia Tools and Applications. 74(6) (2015)2143-55.

[12] O Behnke, K Kröninger, G Schott, T Schörner-Sadenius, Data analysis in high energy physics: a practical guide to statistical methods, John Wiley & Sons. 2013.

[13] M Li, MK Kulhandjian, DA Pados, SN Batalama, MJ Medley, Extracting spread-spectrum hidden data from digital media, IEEE transactions on information forensics and security. 8(7) (2013)1201-10.

[14] L Wei, DA Pados, SN Batalama, RQ Hu, MJ Medley, Optimal multiuser spread-spectrum data hiding in digital images, Security and Communication Networks.8(4) (2015)540-9.

[15] C Yang, F Liu, X Luo, Y Zeng, Pixel group trace model-based quantitative steganalysis for multiple least-significant bits steganography, IEEE transactions on information forensics and security. 8(1) (2013)216-28.

[16] FN Thakkar, VK Srivastava, A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications, Multimedia Tools and Applications. 76(3) (2017)3669-97.

[17] S Nagpal, S Bhushan, M Mahajan, An enhanced digital image watermarking scheme for medical images using neural network, DWT and RSA, International Journal of Modern Education and Computer Science. 8(4) (2016)46.

[18] P Kishore, M Rao, C Prasad, D Kumar, Medical image watermarking: run through review. ARPN J Eng Appl Sci. 11(5) (2016)2882-99.

[19] AK Singh, M Dave, A Mohan, Hybrid technique for robust and imperceptible dual watermarking using error correcting codes for application in telemedicine, International Journal of Electronic Security and Digital Forensics. 6(4) (2014)285-305.

[20] N Venkatram, LS Reddy, PV Kishore, G Fields, GD Vaddeswaram, A Pradesh, Blind medical image watermarking with LWT–SVD for telemedicine applications, Image.(2014)20-23.

[21] L Fan, T Gao, Y Cao, Improving the embedding efficiency of weight matrix-based steganography for grayscale images, Computers & Electrical Engineering. 39(3) (2013)873-81.

[22] B Srinivasan, S Arunkumar, K Rajesh, A novel approach for color image steganography using nubasi and randomized secret sharing algorithm, Indian Journal of Science and Technology. 8.S7 (2015): 228-235

[23] S Arunkumar, V Subramaniyaswamy, B Karthikeyan, P Saravanan, R Logesh, Meta-data based secret image sharing application for different sized biomedical images, Biomedical Research 29 (2018) 394-398.

[24] R Thabit, BE Khoo, A new robust lossless data hiding scheme and its application to color medical images, Digital Signal Processing. 38 (2015)77-94.

[25] G Swain, SK Lenka, A hybrid approach to steganography embedding at darkest and brightest pixels, In Communication and Computational Intelligence (INCOCCI), 2010 International Conference on (2010)529-534. IEEE.

[26] P Sharma, S Shanti, Digital image watermarking using 3 level discrete wavelet transform, Conference on advances in communication and control systems. 24(2013)

[27] D Baby, J Thomas, G Augustine, E George, NR Michael, A novel DWT based image securing method using steganography, Procedia Computer Science. 46 (2015)612-8.

[28] VS Verma, RK Jha, Improved watermarking technique based on significant difference of lifting wavelet coefficients, Signal, Image and Video Processing. 9(6) (2015)1443-50.

[29] NM Makbol, BE Khoo, Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition, AEU-International Journal of Electronics and Communications. 67(2) (2013)102-12.

[30] Z Zhang, L Wu, S Gao, H Sun, Y Yan, Robust reversible watermarking algorithm based on RIWT and compressed sensing, Arabian Journal for Science and Engineering. 43(2) (2018)979-92.

[31] CT Yen, YJ Huang, Frequency domain digital watermark recognition using image code sequences with a back-propagation neural network, Multimedia Tools and Applications. 75(16) (2016)9745-55.

[32] A Mehto, N Mehra, Adaptive lossless medical image watermarking algorithm based on DCT & DWT, Procedia Computer Science. 78 (2016)88-94.

[33] MS Subhedar, VH Mankar, High capacity image steganography based on discrete wavelet transform and singular value decomposition, In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies (2014) 63. ACM.

[34] RA Sadek , SVD based image processing applications: state of the art, contributions and research challenges, arXiv preprint arXiv:1211.7102(2012) .

[35] L Yehia, A Khedr, A Darwish, Hybrid security techniques for Internet of Things healthcare applications, Advances in Internet of Things. 5(03) (2015)21.

[36] MI Khalil , Medical image steganography: study of medical image quality degradation when embedding data in the frequency domain, International Journal of Computer Network and Information Security. 9(2) (2017)22.

[37] Z Wang, AC Bovik, HR Sheikh, EP Simoncelli , Image quality assessment: from error visibility to structural similarity, IEEE transactions on image processing.13(4) (2004)600-12.

[38] S Lyu, H Farid, Detecting hidden messages using higher-order statistics and support vector machines, In International Workshop on Information Hiding (2002)340-354. Springer, Berlin, Heidelberg.

[39] CC Chang, YP Hsieh, CH Lin, Sharing secrets in stego images with authentication, Pattern Recognition. 41(10) (2008)3130-3137.

[40] CC Wu, SJ Kao, MS Hwang , A high quality image sharing with steganography and adaptive authentication scheme, Journal of Systems and Software. 84(12) (2011)2196-207.

[41] HR Kanan, B Nazeri, A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, Expert Systems with Applications. 41(14) (2014)6123-30.

[42] S Arunkumar, V Subramaniyaswamy, KS Ravichandran, R Logesh, RIWT and QR Factorization Based Hybrid Robust Image Steganography using Block Selection Algorithm for IOT devices, Journal of Intelligent & Fuzzy Systems. 2019, 10.3233/JIFS-169984.

Highlights

- Developed a SVD-based secure Image Steganography framework
- Utilized RIWT and DCT for ensuring the better embedding of secret images
- Employed Logistic Chaotic Map to achieve enhanced imperceptibility and security
- Evaluated the developed hybrid steganography approach on UCID benchmark dataset
- Developed scheme is experimentally proven to be better than existing baselines