

ERDH in Medical Images Based on 2-D Compound Transform Domain Technique

G. Nagaraju, P. Pardhasaradhi, V. S. Ghali

Abstract: In the area of data encryption and hiding in colour images, hackers are ready to hack the information which is to be hidden. In this concern it is very important to secure the data by using highly secured reversible data hiding and encryption techniques. The proposed algorithm proposes a new way to image encryption with reversible data hiding (IERDH) scheme with a unique private key in RGB images. A room is allocated in medical image for embedding the data by combining 2-level discrete wavelet transform and 4x4 discrete cosine transform. For any medical images, the patient details are also important to store along with actual image. So these details are imported from excel sheet, and encrypted with the help of carrier image which is generated by special key. This Cipher data image is embedded into allocated transformed image. Combine the individual components to get the transmitted medical image with hidden patient's details. Reverse is possible to restore patient's details from received medical image.

Key words: - reversible data hiding, DWT, DCT, carrier image, data encryption.

I. INTRODUCTION

The digital media and simplicity of the digital systems provide the contents over the digital media highly insecure. Duplication, modification, or even bypass the digital information is easy now a days. It is not possible to avoid hacking the digital information, even though copyright associated with a digital entity. This challenge have accepted from most of the engineers in a big way. Many algorithms or image processing techniques were developed to protect the copyright of digital information. One of the best technique is digital watermarking, and this is the solution to decrease the problem of copyright was addressed elegantly. A secret code or image hidden inside the original image, is used as a digital watermark which claims for the copyright of that image. The "Digital watermarking" is the process where copyright information is embedded invisibly inside the original entity, which is to be protected from the illegal replication and distribution. Encrypting the image and embedding the data with a secret key is a remarkable advantages to overcome digital media insecure.

Revised Manuscript Received on 30 March 2019.

* Correspondence Author

G. Nagaraju*, Ph. D. Scholar, Department of Electronics and communications Engineering, KL University, Vaddeswaram, Guntur Dt., Andhra Pradesh, India.

Dr. P. Pardhasaradhi, Professor in Electronics and Communication Engineering, K.L.University, Vaddeswaram, Guntur Dt., Andhra Pradesh, India.

Dr. V. S. Ghali, Professor in Electronics and Communication Engineering, K.L.University, Vaddeswaram, Guntur Dt., Andhra Pradesh, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](#) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

A. Practical model for Reversible Data Hiding (RDH):

A simple block diagram for general model of reversible data hiding scheme is shown in Figure 1. Here the source image is encrypted with a key and data is embedded with a key to get marked encrypted image. Image encryption is also possible after data hiding. In receiver side three possible ways of retrieving data and original image, one way is original image is recovered using encryption key and the second case is using both encryption and embedded keys, source image and hidden data are retrieved and in the third case only hidden data is extracted using embedded key. This encryption and embedding processes are implemented in several ways.

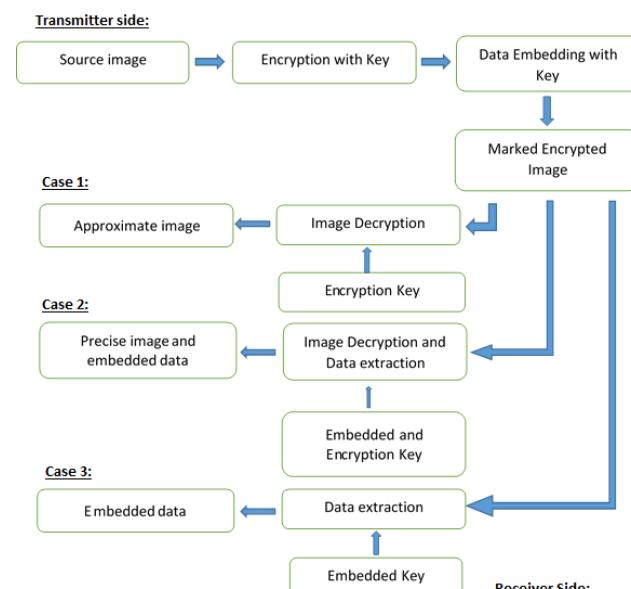


Figure 1: General model reversible data hiding system

An effective crypto-watermarking algorithm is proposed by Hiba Abdel-Nabi et al. [1], where they mentioned how watermarks are embedded in an image with reversible watermarking. And also they proposed another alogorithm [2], a joint reversible data hiding and encryption technique which combines reversible data hiding with high embedding capacity and standard encryption algorithm. The N. Chen et al. [3], proposes a new reversible data hiding method based on the multi-dimensional difference expansions, where they introduced an efficient classification for the expansion schemes and also boundary expandable schemes. To achieve more data inserting and better-quality of stego-image, Rashid Abbasi et al. [4],

proposes a new methodology for reversible and hiding data efficiently using compressed domain with more number of bit planes. Ioan Catalin Dragoi and Dinu Coltuc [5] proposes how to create a room for original and modified pixels after encryption reversible data hiding. Chin-Feng Lee et al. [6], proposed a modification in the multiple-layer embedding method to achieve higher hiding capacity and better image quality for stego-images. To achieve higher PSNR (peak signal-to-noise ratio) values and high embedding rates, Heng Yao et al. [7], proposes a technique of dual-image reversible data hiding using shiftable position method. O. Dorgham et al. [8], proposed a technique which combines symmetric and asymmetric encryption algorithms to make the encryption process secure and faster and which also useful for uploading the medical images on to the web. Houda Chakib et al. [9], proposed an article, where a neural network is implemented for image compression using the feature of wavelet transform. Bikash Debnath et al. [10], proposed an article which introduces an architecture of image steganography using quantum dot cellular automata (QCA) technology. Y. He and Y. Hu [11] presented a paper on watermarking algorithm which combines Discrete Wavelet, Discrete Cosine Transforms and Singular Value Decomposition (DWT-DCT-SVD). Neeru Singla et al. [12], proposes a combination technique of DWT (Discrete Wavelet Transform) and SVD (Singular Valued Decomposition) for the algorithm of watermarking. Singh Arun Kumar [13] presented a new algorithm using discrete cosine transform and discrete wavelet transform, which dealt in hiding a secret picture inside a cover picture utilizing one secret key to generate a stego-image. Mr. Kaushik et al. [14], presented a paper on image watermarking techniques which is based on hybrid watermarking. W. Yang et al. [15], presented a paper which predicts pseudo computed tomography (pCT) images from T1 and T2-weighted magnetic resonance imaging (MRI) data. Shehab et al. [16], proposes a new watermarking-based scheme for image authentication and self-recovery for medical applications. O. Kwon, S. Choi and B. Lee [17] proposes a watermark-based forgery detection method for authenticating JPEG image integrity in the frequency domain. M. Preishuber et al. [18], presented paper which shows chaos-based image encryption. A. Abd El-Latif et al. [19], proposed a quantum steganography approach which hides a quantum secret image into a quantum cover image. Zhuoqian Liang et al. [20], presented a blind image watermarking scheme, which chooses the concept of histogram-based embedding.

The next topics of this paper are organized as follows: Section 2 discusses relative work of DWT, DCT, Carrier image generation using secret key, importing patient details from excel sheet and embedding the data in image. Section 3 introduces the explanation of proposed algorithm in detail. Section 4 shows the simulation results. Finally, section 5 gives conclusion.

II. RELATED WORK

A. Carrier image Generation

Carrier image is generated by secret alpha-numeric key with the help of ASCII codes. Here we used different 8-bit ASCII codes for different key words. This code is made basically for indicating all symbols, integers and numbers. There are 65 possible combinations of the ASCII hexa decimal code and which the binary form of hexa-decimal code is assigned to each character. Total 26 alphabets (uppercase letters), 26 alphabets (lowercase letters), 10 decimal numbers (from 0 to 9) and 3 special characters (space, comma, full stop) forms to give 65 alphanumeric characters. A unique code is assigned to each alphanumeric character by using ASCII code. After entering the alpha-numeric key, by using 8-bit ASCII codes this key is converted into decimal values later binary values. As we enter the different patient details, each character in details are converted into binary form using ASCII codes and they are rearranged in a matrix form of which size is equal to the size of 64 x 64 image. If the length of the patient details is very small, those details are repeated till the length will become equal to size of 64 x 64 image. With these binary values a black and white (i.e. 2bit) carrier image is generated. The carrier image is very useful to convert patient details into cipher data.

B. Importing patient details

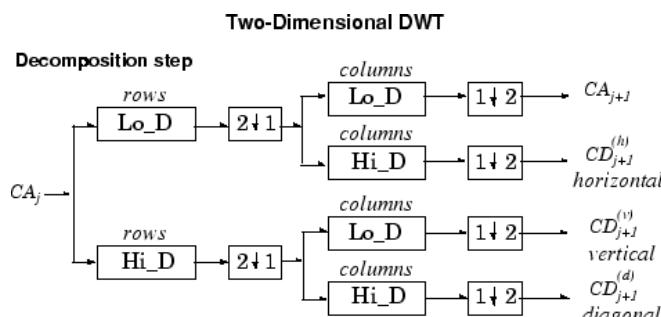
The data to be embedded in the source image, is the combination of six different patient's information fields like patient's gender (1 character), patient's age (2 characters), patient's name (50 characters), patient's location (25 characters), patient's ADHAAR number (12 characters) and patient's contact number (10 characters). These six components are generated by using ASCII codes and converted into binary form and concatenated into a binary vector w of 800 bits (100 characters). Each character will be having a unique 8bit value generated by ASCII code. With this newly generated vector w , a 64 x 64 vector matrix is generated and it is added with carrier image which is generated by secret key to obtain cipher image. To get original patient's information, at the decoder side inverse permutation will be performed

C. Discrete Wavelet Transform

DWT is used in several variety of signal and image processing applications, such as in video and audio compression, noise removal in audio, and in wireless antenna distribution simulations. The 2-D discrete wavelet transforms (DWT) decomposes the image into 1 approximation and 3 details. The approximation image looks just like the original but it is only 1/4th scale of the original. Combination of 1-D DWT in both the horizontal and the vertical directions gives two dimensional DWT. An image is separated into horizontal (HL), vertical (LH), diagonal (HH) detail components and a lower resolution approximation image (LL) by using DWT.



The process of decomposing image into 3 details and 1 approximation is shown in Figure 2. Generally the wavelet transform splits a signal into low pass and high pass sub band signals. Therefore high energy watermarks can be embedded in the high frequency regions such as the high-resolution LH, HL, and HH detail bands. Image quality is not effected with embedding watermarks in these regions and also increases the robustness of watermark methodology.



Where
 $\boxed{2\downarrow 1}$ Downsample columns: keep the even indexed columns
 $\boxed{1\downarrow 2}$ Downsample rows: keep the even indexed rows
 $\boxed{\text{rows}}$
 \boxed{X} Convolve with filter X the rows of the entry
 $\boxed{\text{columns}}$
 \boxed{X} Convolve with filter X the columns of the entry

Initialization $CA_0 = s$ for the decomposition initialization

Figure 2: Decomposition steps of image using Two-Dimensional DWT

D. Discrete Cosine Transform

DCT represents data in frequency domain rather than spatial domain. Spatial domain watermarking techniques are somewhat weak when compared with DCT based watermarking techniques. DCT based techniques are used in the applications of low pass filtering, brightness and contrast adjustment, blurring etc. However, DCT techniques are computationally expensive and implementation is also difficult. These techniques are weak at geometric attacks like rotation, scaling, cropping etc. Global based DCT and Block based DCT are two classifications in DCT domain watermarking. The two-dimensional discrete cosine transform is the combination of one-dimensional DCT followed by another one-dimensional DCT. Two-dimensional DCT for an input image A and output image B is given as

$$B_{pq} = \alpha_p \alpha_q \sum_{n=1}^{M-1} \sum_{m=1}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad 0 \leq p \leq M-1, \quad 0 \leq q \leq N-1$$

Where $\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p=0 \\ \frac{1}{\sqrt{M}}, & 1 \leq p \leq M-1 \end{cases}$, $\alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q=0 \\ \frac{1}{\sqrt{N}}, & 1 \leq q \leq N-1 \end{cases}$

Where M and N variables are the sizes of image A.

E. Embedding the data in image

Patient's details are extracted from excel sheet and construct a 64 x 64 vector matrix from data. To get Cipher data this

matrix is EXORed with another 64 x 64 carrier image which is generated by using unique secret key. This 64 x 64 cipher image is subtracted by 64x64 DC component matrix which is generated from original source image, so the resultant is the DC component matrix. Inserting these DC values back into the each 4x4 sub block. Taking the IDCT of each 4x4 sub block. Re-joining the embedded 4x4 blocks to form new LL component. Taking the IDWT using the new LL component. Combine the G and B components with this R component to get the final Encrypted Reversible Data Hidden (ERDH) image. In the same way in our 256 x 256 image there is a possibility of 1536 characters can embed by using all R, G, B components. In each component up to 512 characters are embedded.

III. PROPOSED METHODOLOGY

Schematic representation of our proposed algorithm is shown in Figure 3.

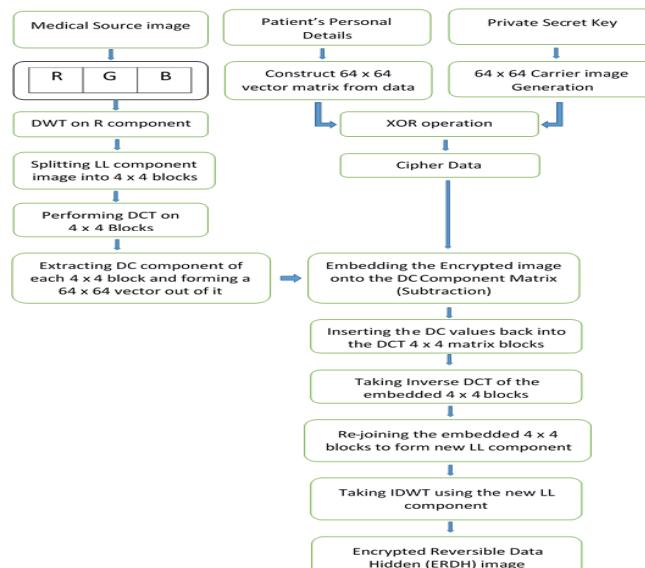


Figure 3: Block diagram for designing proposed technique

Brief Explanation

The step by step flowchart for the proposed scheme is described in following steps:

Step 1: Initially red (R), green (G) and blue (B) components are extracted from the original colour medical image. The dimensions for the image are 256 x 256.

Here the values are shown for the R component of original Image (Consider only first 5 x 5 elements)

255	250	254	254
255	252	249	252
255	255	252	253
250	245	254	251



Step 2: A 2 level 2D-DWT is applied on R colour component to get four frequency sub-bands. The values for LL component are shown as (Consider only first 5 x 5 elements)

506	504.5	507.5	504.5	509
502.5	505	382.5	357	356
503	505.5	103.5	71	67
506	505	110.5	91	92
507.5	506.5	112	91	90

Step 3: By considering the LL component and divide it into 4x4 sub-blocks. Here only first 4 x 4 block values are shown as

506.00	504.50	507.50	504.50
502.50	505.00	382.50	357.00
503.00	505.50	103.50	71.000
506.00	505.00	110.50	91.000

Step 4: Apply the DCT to each block of LL component in R colour component. The first 4 x 4 block values are shown as

1540.25	448.6148	-20.75	-164.71569
340.88765	-317.85334	6.4999858	124.97718
76.25	-70.58393	10.75	21.660076
-74.633168	69.477182	0.0135982	-28.646663

Step 5: The 64x64 DC component matrix is obtained by converting the DC component vector that is generated by extracting the DC component of each 4 x 4 sub block. The values are shown only for first 5 elements)

1541.25	1023.5	1024	1024	1024
---------	--------	------	------	------

Step 6: Patient's details are extracted from excel sheet and construct a 64 x 64 vector matrix from data.

205 (for number '5') - 11001101

Step 7: To get Cipher data this matrix is EXORed with another 64 x 64 carrier image which is generated by using unique secret key.

62 (for letter 'y') – 111110

1	0	1	1	0	0	1	1
0	1	1	1	1	1	0	0
1	1	0	0	1	1	1	1

Converting 64 x 64 cipher Image into vector Matrix (the values shown only for first 8 elements)

1	1	0	0	1	1	1	1
---	---	---	---	---	---	---	---

Step 8: By subtracting the 64x64 cipher image with a 64 x 64 DC component matrix results the new DC component matrix. The first 5 values are shown as

1540.25	1023.5	1023	1024	1024
---------	--------	------	------	------

Step 9: Inserting the DC values back into the each 4x4 sub block.

Step 10: Taking the IDCT of each 4x4 sub block.

Step 11: Re-joining the embedded 4 x 4 blocks to form new LL component and the corresponding values for first 4 x 4 block are shown as

505.75	504.25	507.25	504.25
502.25	504.75	382.25	356.75
502.75	505.25	103.25	70.75
505.75	504.75	110.25	90.75

Step 12: Taking the IDWT using the new LL component. The below values are shown for first 4 x 4 block R component of the output image.

254.875	249.875	253.875	253.875
254.875	251.875	248.875	251.875
254.875	254.875	251.875	252.875
249.875	244.875	253.875	250.875

Step 13: Combine the G and B components with this R component to get the final Encrypted Reversible Data Hidden (ERDH) image. Here the used source image having the dimensions of 256 x 256. In this 256 x 256 image there is a possibility of embedding 1536 characters by using all R, G, B components. In each component up to 512 characters are embedded. By applying the same methodology on Green and Blue components, we will insert another 1024 characters. In the reverse process, by using original source image and secret key, we will get the same information which is hidden in the received image. Take the source image and splits it into R, G, and B components and apply DWT and DCT to get a 64 x 64 DC component matrix. With secret key a 64 x 64 binary carrier image is generated. By applying EXOR operation on DC component matrix and binary carrier image, a 64 x 64 vector matrix is generated. By using this 64 x 64 vector matrix the data which is hidden in received image is retrieved. By observing the input source image and output image, the hiding bpp rate is 0.024 and the PSNR for this algorithm is infinity.

IV. SIMULATION RESULTS

Here the results are shown for the proposed algorithm. reversible data hidden image. Initially Figure 4. shows the input medical image and the output ERDH (Encrypted Reversible Data Hidden) image. This input image is splits into R, G, and B components, and to get approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components, discrete wavelet transform is applied on R component. These results are shown in Figure 5.

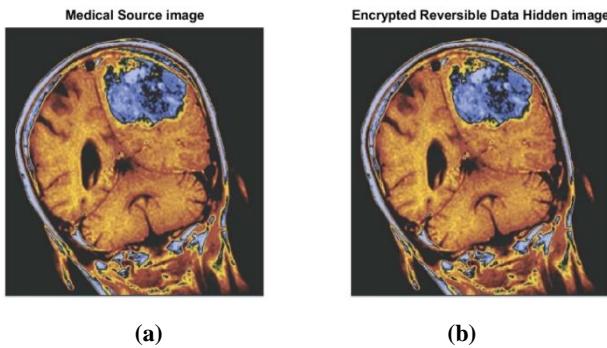


Figure 4: (a) Medical Source Image
(b) Encrypted Reversible Data Hidden Image

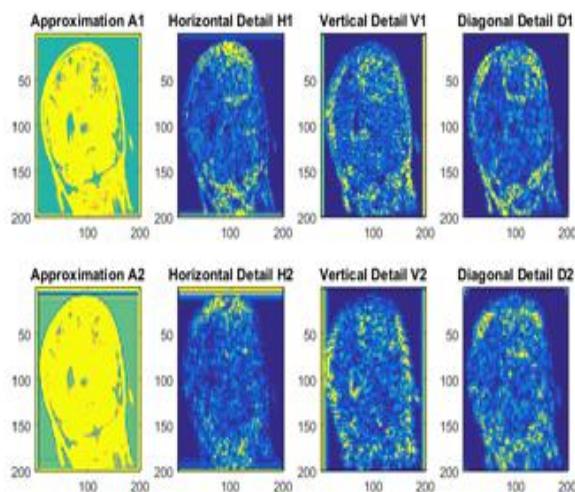


Figure 5: First level Decomposition of R component into approximation and detail components

The second level wavelet decomposition of R component into approximation and detail components are shown in Figure 6. Here A1 approximation coefficients, H1 horizontal detail coefficients, V1 vertical detail coefficients, and D1 diagonal detail coefficients are first level decomposition components.

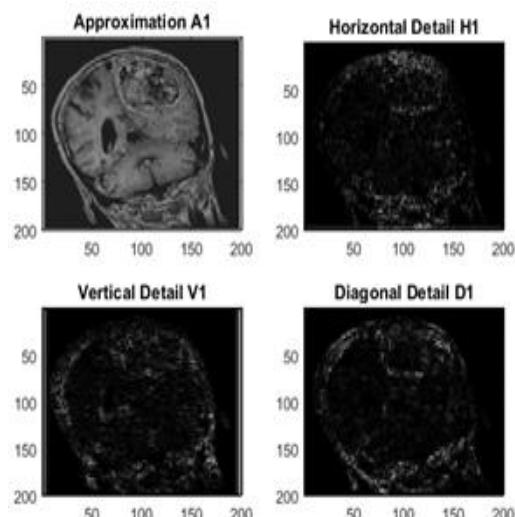


Figure 6: Second level Decomposition of R component into approximation and detail components (color mapped)

In the same way A2 approximation coefficients, H2 horizontal detail coefficients, V2 vertical detail coefficients, and D2 diagonal detail coefficients are second level decomposition components. Example Patient details are shown in Figure 7. These details are extracted from excel sheet and converted into binary to form a 64 x 64 binary matrix. By using these patient details in binary form, generate a 64 x 64 vector image and it is shown as Figure 8(a). A carrier image which is shown in Figure 8(b) is generated by using a secret key, here it is “My date of birth is September 4th 2010.”

Figure 7 shows a screenshot of Microsoft Excel displaying patient details in a spreadsheet. The details include gender (M), age (55), name (N. T. Rama rao), location (Guntur), Aadhar number (8888 6666 4444), and contact number (98489 84898). The table is located in the range A1 to E6.

Figure 7: Patient Details

This alpha-numeric key is converted into decimal by using ASCII codes later into binary. Adding these vector and carrier images results Cipher image which is shown in Figure 9. This Cipher image is subtracted from DC component matrix which is generated from source image. From reconstructed image, by reverse process with the same secret key gets the hidden information on command window which is shown in Figure 10.

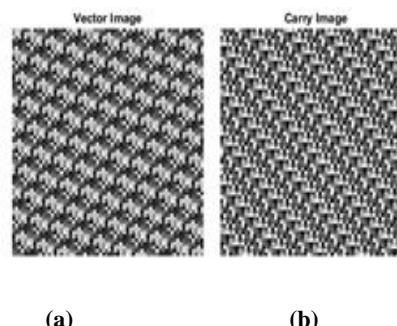


Figure 8: (a) 64 x 64 vector matrix from patient details
(b) 64 x 64 carrier image with key “My date of birth is September 4th 2010.”

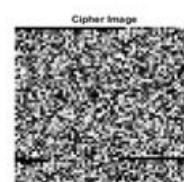


Figure 9: Cipher image

ERDH in Medical Images Based on 2-D Compound Transform Domain Technique

```
MATLAB Command Window
press any key for decryption
GENDER = M
AGE = 55
NAME = N. T. Rama rao
LOCATION = Guntur
ADHAR_NUMBER = 000066664444
CONTACT_NUMBER = 9848984898
>>
```

Figure 10: Retrieved Patient details

V. CONCLUSION

The way of hiding the data in image is so simple and reversible in this proposed algorithm. Even though the bits per pixel (bpp) rate is quite low i.e. 0.024, and its peak signal to noise ratio (PSNR) is infinity. The hidden data is extracted only when receiver having both original source image and secret key. So hackers are unable to hack the information which is hidden. By combining DWT, DCT and carrier image generation techniques, this proposed algorithm has tremendous advantages in implementation. Here only 800 bits information was added, but it is possible to add up to 12288 bits of information by using this technique. This algorithm is extended to add information which is related to corresponding medical image. By analysing the Medical image (MRI, CT, X-ray, and Ultra-sound images), the medical information or disease details of the patient like the type and grade of tumor, location of the tumor in brain, its Size, other Health Conditions, preferred Treatment, Doctor's Name, hospital name and Dated on etc., are extracted. Apart from personal information of the patient, these medical information is also embed into the corresponding medical source image. By assigning a unique tag to each image, it is possible to upload into cloud. With this there is a possibility of achieving to retrieve the patient's medical image and corresponding medical information and personal information wherever and whenever.

REFERENCES

- 1 Hiba Abdel-Nabi, Ali Al-Haj, "Efficient Joint Encryption and Data Hiding Algorithm for Medical Images Security", IEEE 8th International Conference on Information and Communication Systems (ICICS), 11 May 2017, PP: 147-152, doi: 10.1109/IACS.2017.7921962.
- 2 H. Abdel-Nabi and A. Al-Haj, "Medical imaging security using partial encryption and histogram shifting watermarking", 2017 8th International Conference on Information Technology (ICIT), Amman, 2017, PP: 802-807. doi: 10.1109/ICITECH.2017.8079950
- 3 N. Chen, S. Zhou, C. Cheng and C. Su, "Reversible Data Hiding for Medical Images Using Boundary Expandable Schemes", 2018 IEEE Seventh International Conference on Communications and Electronics (ICCE), Hue, 2018, PP: 335-339. doi: 10.1109/CCE.2018.8465710.
- 4 Abbasi, R., Luo, B., Rehman, G. et al. Vietnam J Comput Sci (2018) 5: 185. <https://doi.org/10.1007/s40595-018-0114-z>
- 5 I. C. Dragoi and D. Coltuc, "Reversible Data Hiding in Encrypted Images Based on Reserving Room After Encryption and Multiple Predictors," 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, 2018, PP: 2102-2105. doi: 10.1109/ICASSP.2018.8461362.
- 6 C. Lee, J. Ji Shen and Y. Hua Lai, "Data Hiding Using Multi-Pixel Difference Expansion," 2018 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, 2018, PP: 56-60. doi: 10.1109/CCOMS.2018.8463244.
- 7 Heng Yao, Chuan Qin, Zhenjun Tang and Xinpeng Zhang, "A general framework for shiftable positionbased dual-image reversible data hiding", Volume 2018, Issue 41, pp. 1-10, 6 June 2018, <https://doi.org/10.1186/s13640-018-0281-y>.

8 O. Dorgham, , Jordan Banan Al-Rahamneh, , Jordan Ammar Almomani, Irbid, Jordan Moh'd Al-Hadidi, Jordan Khalaf F. Khatatneh, "Enhancing the Security of Exchanging and Storing DICOM Medical Images on the Cloud", International Journal of Cloud Applications and Computing, Volume 8, Issue 1, January-March 2018, PP: 154-172, DOI: 10.4018/IJCAC.2018010108.

9 Houda Chakib, Brahim Minaoui, Abderrahim Salhi, Imad Badi, "Switching of Wavelet Transforms by Neural Network for Image Compression", Journal of Electronic Commerce in Organizations Volume 16 • Issue 1 • January-March 2018, PP: 43-56, DOI: 10.4018/JECO.2018010104.

10 BikashDebnath, Jadav ChandraDas, DebasishDe, "Design of image steganographic architecture using quantum-dot cellular automata for secure nanocommunication networks", Elsevier journal of Nano Communication Networks, Volume 15, March 2018, Pages 41-58, DOI: 10.1016/j.nancom.2017.11.001.

11 Y. He and Y. Hu, "A Proposed Digital Image Watermarking Based on DWT-DCT-SVD," 2018 2nd IEEE Advanced Information management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, 2018, pp. 1214-1218. doi: 10.1109/IMCEC.2018.8469626.

12 Neeru Singla, Dr. Rajbir Kaur, "DWT-SVD based Watermarking Algorithm for the Protection of Ownership of an Image", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072, PP: 4264-4266.

13 Singh Arun Kumar, Singh Juhi and Singh Harsh Vikram, "DCT- and DWT-Based Intellectual Property Right Protection in Digital Images", First International Conference on Artificial Intelligence and Cognitive Computing, Advances in Intelligent Systems and Computing 815, https://doi.org/10.1007/978-981-13-1580-0_49, PP:507-513.

14 Mr. Kaushik H. Raviya, Dr. Ashish M. Kothari, "Comparative Study of Digital Image Watermarking Based I.J.Cox's Algorithm versus proposed Hybrid DWT-DCT Approach", European Journal of Academic Essays 5(5): PP: 98-104, 2018.

15 W. Yang et al., "Predicting CT Image From MRI Data Through Feature Matching With Learned Nonlinear Local Descriptors," in *IEEE Transactions on Medical Imaging*, vol. 37, no. 4, pp. 977-987, April 2018., doi: 10.1109/TMI.2018.2790962.

16 Shehab et al., "Secure and Robust Fragile Watermarking Scheme for Medical Images," in *IEEE Access*, vol. 6, pp. 10269-10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

17 O. Kwon, S. Choi and B. Lee, "A Watermark-Based Scheme for Authenticating JPEG Image Integrity," in *IEEE Access*, vol. 6, pp. 46194-46205, 2018, doi: 10.1109/ACCESS.2018.2866153.

18 M. Preishuber, T. Hütter, S. Katzenbeisser and A. Uhl, "Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2137-2150, Sept. 2018, doi: 10.1109/TIFS.2018.2812080.

19 A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri and B. B. Gupta, "Efficient Quantum Information Hiding for Remote Medical Image Sharing," in *IEEE Access*, vol. 6, pp. 21075-21083, 2018, doi: 10.1109/ACCESS.2018.2820603.

20 Zhuoqian Liang, Bingwen Feng, Xuba Xu, Xiaotian Wu and Tao, "Geometrically Invariant Image Watermarking Using Histogram Adjustment"International Journal of Digital Crime and Forensics (IJDCF) 10(1), 2018 [Pages: 13, DOI: 10.4018/IJDCF.2018010105.

AUTHORS PROFILE



Naga Raju, Presently working as assistant professor in Dept. of ECE, S.R.K.R. Engineering College, Bhimavaram, AP, India. He received B.Tech degree from S.R.K.R Engineering College, Bhimavaram in 2012, and M.Tech degree in Computer electronics specialization from Govt. College of Engg., Pune University in 2004.



Published By:

Blue Eyes Intelligence Engineering
& Sciences Publication

Presently he is pursuing Ph. D. in Department of ECE, KL University, Vaddeswaram. His current research interests include Image processing, digital security systems, Signal processing, Biomedical Signal processing, and VLSI Design.



Dr. P. Pardha Saradhi, He was born in India, A.P, in 1978. He received UG, PG and Ph.D degrees from Acharya Nagarjuna University, A.P, India in 1998, 2000 and 2012 respectively. From June2000-Jan2012 he worked as lecturer in Hindu College, Machilipatnam, from Jan2012 to Feb2014 worked as Associate Professor in Sri Vasavi institute of engineering and technology, Nandamuru and 2014 to till date he is working as Professor in Electronics and Communication Engineering, K.L.University, Vaddeswaram. He has published 67⁺ papers in International journals. He is reviewer for several international journals including Elsevier and Taylor and Francis and served as Coordinator and co-chair for Spaces-2018 IEEE international conference. His research interests include antennas, liquid crystals, LC antennas, Image processing. He is a life member of IACSIT, IAENG, UACEE and IIRJC. He is the editorial board member for many indexed journals.



Dr. V S Ghali, He received his M.Sc. degree in Electronics from Acharya Nagarjuna University, Guntur, India, in 1998 and the M.E. degree in Applied Electronics from Satyabama University, Chennai, India in 2008. He received his Ph.D. degree in ECE from IIITDM, Jabalpur, India in 2013. He is a recipient of Research award from University grant commission, India in 2014. Currently he belonged to Infrared Imaging Center and also professor in ECE, College of Engineering, K.L.University, Vaddeswaram, Andhra Pradesh, India.