International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.04, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Hybrid Transform Domain Based Secure and Robust Watermarking Technique forPrivacy for Medical Applications

Nasir N. Hurrah, Nazir A. Loan, Shabir A. Parah and Javaid A. Sheikh

Department of Electronics and Inst. Technology, University of Kashmir, India.

ABSTRACT

The massive increase in the exchange of the digital content through different communication channels has given rise to increasing security issues including threats to privacy, data integrity and copyright protection. The watermarking has proved to be most resilient technique to preserve the data privacy and security. Digital watermarking is the technique of hiding digital information in a multimedia file like text, image, audio, video etc. such that observer shall not be able to extract the secret information without knowledge of the watermarking algorithm. In this paper a new robust watermarking scheme is proposed for gray scale images. The proposed method has been implemented in hybrid transform domain through use of Discrete Cosine Transform (DCT), Integer Wavelet Transform (IWT) and Singular Value Decomposition (SVD). The use of three transform domain techniques provides the watermark a very high robustness against any kind of signal processing and geometric attack. In addition to robustness the watermark has been made highly secure by using the encryption technique such that even in extreme cases if the unauthorized user cracks the embedding algorithm no meaningful information will be extracted.The results achieved through proposed scheme demonstrate high level of robustness and security of the watermark against different kinds of modifications and outperforms latest state of art techniques.

Keywords*—Discrete Cosine Transform (DCT), Discrete WaveletTransform (DWT), Singular Value Decomposition (SVD), Robustness, Image authentication,Security.*

1. INTRODUCTION

The worlds approach to health is broken but that is slowly changing. Medical data doubles every three years and the seven trillion-dollar health industry is unable to keep up with the staggering rate at which information is produced from medical records, clinical trials and research to personal fitness band, implanted devices and sensors that collect real time data. Each of us can generate the equivalent of 300 million books of health related data in our lifetime. In fact, approximately 35 cents of every dollar spent on medical is wasted and yet there is a reason for hospitals, doctors and patients alike to be optimistic about the future. Taking this in consideration the IBM has built the Watson health cloud which brings together vast amounts of medical data into one centralized

thinking hub on the cloud combining traditional analytics with the advanced cognitive capabilities. The ability to learn and overtime refine its analysis is based on what it is learning to turn this wealth of data into knowledge. Watson health clouds ecosystems combines massive amounts of data and knowledge and brings together researchers, doctors, patients, pharmaceutical companies and insurers in a secure and open platform **[1, 2].** Medical privacy is one of the key factors which a patient is worried about as most of the patient information is stored in the cloud. As the knowledge base continues to grow, apps built using the Watson health cloud unable researchers, doctors and pharmaceutical companies to drive medical advancements and improve patient outcomes. Physicians can be more confident and accountable in treatments and individuals can be more responsible for their own health and wellness by taking preventive action. IBM Watson healthcare cloud is rapidly transforming healthcare around the world and its advanced cognitive capabilities, interactive ecosystem and secure de-identification dramatically change the dynamic between patients, doctors and the medical community creating a brighter healthier future for all. Even though lot of measures are being taken out currently in order to keep the privacy content intact lot of procedures require transmission of one's private information through insecure channels. This creates the need for state of art procedures to keep the private information safe and intact.

The data vulnerability exchanged through different networks like internet has recently gained a rapid rise due to the readily available state of art hacking and editing software's and tools**[3-7].** The need for strong anti-piracy, anti-theft and anti-hacking has hence proportionally increased as the information exchange through different channels has proven to be best and easy method. The transmission of different multimedia files including text, image, audio and video over these non-secure mediums has forced users and owners to invest large amount of money on security. As the senders ensures that the transmission is secure, the legitimate receivers also put lot of caution for ensuring what they receive is original and not manipulated. For ensuring this data safety different precautionary measures are taken by the designers and researchers**[8-12].** Data integrity and authentication have been one of the major concerns of the researchers for ensuring safe data exchange and hence preserving the privacy and copyright protection. This is done by pre-processing and modifying the information before any usage or exchange through insecure networks. These modifications may include some of the signal processing operations like data compression, filtering, equalization and many other geometric operations.Clearly, the effect of these operations results in some quality reduction and addition of redundancy but the actual information content remains intact. Standard security procedures are effective in keeping the data secure but not able to resist the all kind of manipulations up to an efficient level.Watermarking is a technique of hiding the secret information in a cover media in such a manner that there no visible perceptual quality degradation of the host media. The image to which another image is hidden is the cover image or original image and the hidden image is known as watermark.

The authentication requirement in case of highly sensitive applications puts a smaller threshold limit ascompared to applications which are less critical and authentication requirements are met bychoosing a value forthreshold which is comparably much higher. However, no compromise can be made with security in any case and the algorithm should be capable of detecting any kind of modification in the received content which being exchanged**[13-17].**In comparison to other multimedia images the medical images are more sensitive as

patientinformation is contained in them which is crucial for diagnosis and treatment of diseases. Hence greater privacy and security is required for them as a minute alteration in medical data can avail wrong results which can prove fatal for patient's health**[18-22].** Hence, e-health care applications require better security and integrity for medical images while transmission through any insecure channel.

In this paper a robust watermarking scheme has been proposed with high level securityin order to ensure the originality and authenticity of the embedded data while being received. This is done by scrambling the secret data to be embedded via a unique key followed by embedding of this encrypted data by modifying the transform domain coefficients of the cover image.In addition to security and robustness, image authentication is also one of the key factor for determining efficiency of a watermarking scheme and the application determines the required values for each.

2. LITERATURE REVIEW

Research on data hiding has abruptly increased many folds in recent years due transmission insecurity of sensitive information exchanged through different insecure networks. Also, the ever increasing challenges faced by different multimedia industries for securing their data has kept research on data hiding an area of huge interest from researchers throughout the globe.There are predominantly two techniques used for data hiding, watermarking and steganography. The steganography involves embedding private data or watermark into the cover media such that no one can get a meaningful message before using an algorithm meant for extracting it. As systems using steganographic technique transmit encrypted data it poses a doubt in the minds of an unauthorized user about the importance of the message received and hence the attacker tries different tools to get the private information from the data. Watermarking instead deals with hiding the secret message in a host media in such a manner that there is almost no change in geometry or perceptual quality of the host media. This proves to be of great advantage as anyone who receives the data does not get any clue of the importance of the information content within. Hence watermarking proves to be more secure to any adversaries as compared to steganography. The data hiding techniques are broadly categorized into two groups; Spatialdomain technique and transform domain technique. While as watermark is embedded directly in the original pixels of the host image in spatial one, the transform domain technique involves hiding of watermark in the frequency domain coefficients. These coefficients are obtained by applying a transform like DCT, Stationary Wavelet Transform (SWT), IWT, DWT etc. on the host image. Spatial domain techniques mostly modify the Least Significant Bit (LSB) of a pixel according to the watermark bits and used techniques like SVD for ensuring robustness of algorithm. The major weakness of spatialdomain techniques is that they are less resilient to various signal processing, compression and geometric attacks. Due to this reason the spatial domain techniques are unsuitable for applications having robustness a key requirement and as such the spatial domain techniques are mostly used for authentication purposes.The transform domain based data hiding techniques shows great robustness against any kind of data manipulation and theft attack from an external unauthorized agency at the cost of some increase in design complexity [23-25].

A robust watermarking technique has been presented in **[26] and is** based on difference of corresponding coefficients between two successive DCT blocks. The host image is first splitted into 8x8 blocks followed by application of DCT on each block. Based on the difference between two corresponding coefficients of

neighbouring blocks watermark embedding is carried out. The technique shows ample amount of robustness againstdifferent attacks like cropping, rotation, JPEG Compression and some other singular attacks. But the drawback of the scheme is that it lacks the procedure touse all the DCT blocks for embedding the watermark and hence embedding capacity is low. The technique has been improved and a better embedding capacity has been achieved in **[27].**ADCT domain based blind watermarking scheme for embedding more than one watermark in a color image has been proposed in **[28]**. The proposed technique utilizes the concept of repetition code foraccurate extraction of the watermark bits which is ensured by modification of some of the mid frequency coefficients at the embedding stage. Arnold transform has been used for encrypting the watermark before embedding which ensures high level of security. The imperceptibility and robustness of the scheme is satisfactory but the computational complexity is high. A DWT and DCT based robust watermarking schemefor medical images is proposed in **[29]**. After splitting the cover image into two regions (ROI and RONI) multiple watermarks (image and text) are embedded in them. Rivest-Shamir-Adleman (RSA) encryption technique has been used in order to increase the security of watermark.Lifting Wavelet Transform (LWT) has been used for implementation of robust and blind watermarking scheme **[30].**The scheme uses the energy compaction property of LWT and a block selection procedure to obtain high image distortion tolerance and greater security over conventional techniques. The proposed scheme provides good security but offers lesser payload. One of the main drawbacks of the proposed scheme is that it underperforms in case of rotation, average filtering, and salt and pepper noise attacks.

A secure watermarking scheme for gray scale images has been reported in **[31]**. Although, security of the watermark has been ensured through encryption, the robustness of this technique against various signal processing attacks is not up to the mark. A highly secure and blind watermarking scheme is proposed in **[32]**. The security has been ensured through application ofArnold Transform. Although security and robustness is good the scheme offers low imperceptibility and payload. An image encryption scheme using concept of chaotic maps, nonlinear inter-pixel computing and swapping based permutation approach has been proposed in **[33]**. The proposed scheme offers advantage that it can be used for both medical and standard images. The watermarking scheme shows better security due to the use of encryption technique. A block based robust medical image encryption scheme using chaotic cat maps has been presented **[34]**.The concept of block mixing has been used to resist the statistical and differential attacks.A new method for robust image watermarking is proposed in this paper aimed for data privacy and copy protection. The purpose of this robust image watermarking scheme is to ensure that the received watermarks are intact even if data undergoes several attacks.

3. PROPOSED SCHEME

In this section, the proposed watermarking algorithm is explained in detail starting with the embedding up to extraction. The proposed scheme is a robust watermarking technique for copyright protection and data privacy purposes based on hybrid transform domain. The work proposes a block based image watermarking algorithm which uses cryptographic algorithm to find out the positions of the cover image in which the watermark is to be embedded. For the scheme, to ensure high level security, encryption algorithm has been applied on the watermark before embedding process.

3.1 Embedding Algorithm

The proposed technique is aimed to provide better performance in terms of security, imperceptivity and robustness against different attacks. The proposed scheme is blind and watermark is embedded in hybrid transform domain after encrypting it with the chaoticmap. The generalized flow diagram of the proposed scheme has been shown in Fig 1.

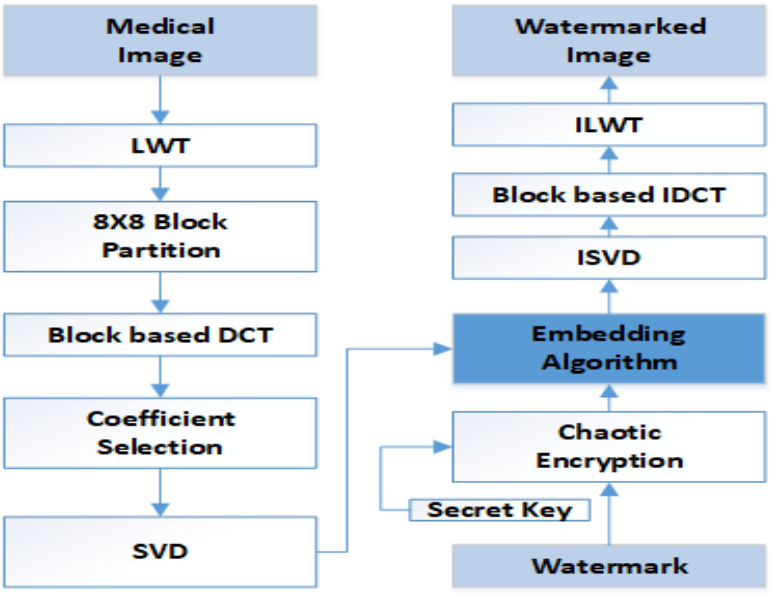


Fig. 1. Block diagram for embedding watermark

The watermark embedding process starts with an encrypted watermark (which generally is a binary logo of size 32 x 32) and a cover image of size 512 x 512. The robust watermark has been embedded using the following steps:

Step 1: Use chaotic map technique to encrypt the watermark to be embedded.

Step 2: Apply Integer wavelet transform on the host cover image.

Step 3: Choose one of the components of the IWT and divide it into 8 x 8 blocks. On each of these 8x8 blocks DCT is applied.And from each of the 8x8 block eight mid frequency coefficients are chosen and arranged into two 2x2 blocks, M_1 and M_2.

Step 4: Apply SVD on M_1 and M_2. Before staring embedding process, the mean of first element of 2x2 block and first element of second 2x2 block is calculated. The mean is stored in variable, '$\prod_X$'.

$$M = U*S*V \qquad (1)$$

Step 5: The watermark bit is embedded by modifying the vales of $M_1(1)$ and $M_2(1)$ using the steps described in Fig. 2.

Step 6: Before starting the embedding process three variable are initialized which also act as secret keys. These variables are μ, β and α. If w(x) is the xth watermark bit, then embedding is done as follows:

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.04, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

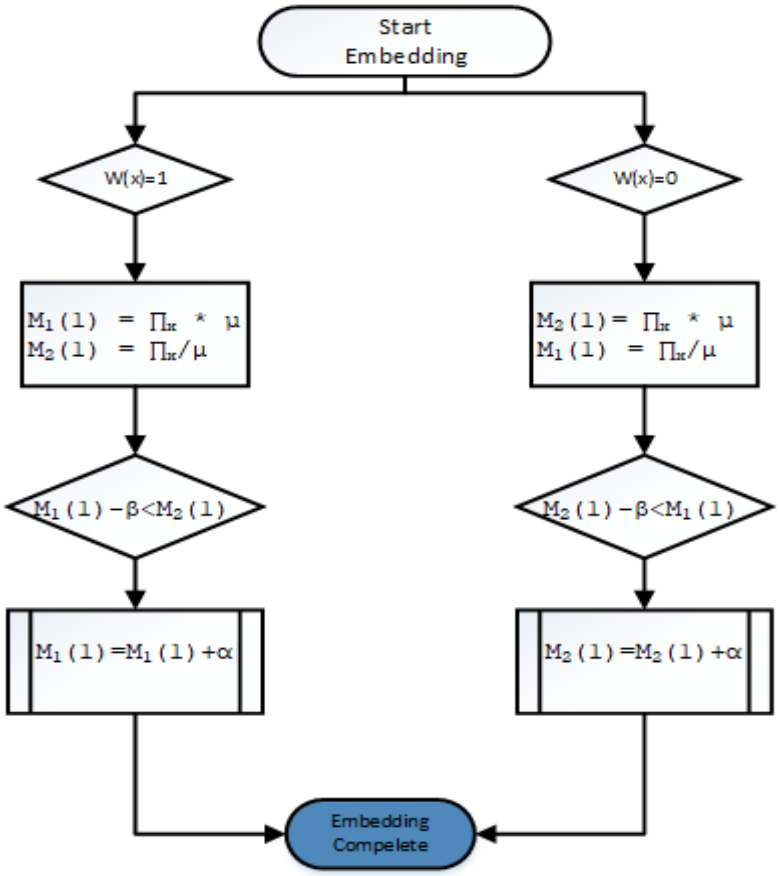


Fig. 2. Algorithm for embedding a watermark bit in a block

Step 7: After embedding process is complete the two 2x2 blocks SVD is applied again as per following equation:

$$M' = U*S*V^T \qquad (2)$$

Step 8: The resulting 2x2 blocks in step 6 replace the corresponding coefficients in the 8x8 block from which they were extracted. This is followed by applying IDCT on the 8x8 block and then application of inverse IWT to get final watermarked image.

3.2 Watermark Extraction

The extraction process used in robust watermarking is inverse of corresponding embedding process. After doing some necessary pre-processing of the watermarked image the resulting watermark logo is obtained. After obtaining the 2x2 blocks as per the steps shown in Fig. 1, i.e., M_1' and M_2' watermark bit is extracted using the following equations:

$$\text{If } M_1'(1) > M_2'(2),\ w(x) = 1 \qquad (3)$$

$$\text{If } M_1'(1) < M_2'(2),\ w(x) = 0 \qquad (4)$$

4. EXPERIMENTAL ANALYSIS

In this section, subjective and objective quality metrics obtained from the proposed algorithm are presented. Several standard medical and gray scale host cover images of size M x N like brain, hand, lena, peppers, plane, etc. have been used for evaluation and experimentation of the proposed scheme. Various test images (512 x 512) and watermark (32 x 32) have been used for the analysis are shown in Fig. 3. To evaluate the imperceptivity of the watermarked image, the parameter PSNR and SSIM are used. Similarly, parameters like Bit error rate (BER) and Normalized Cross correlation (NCC) are used for testing the fragility.

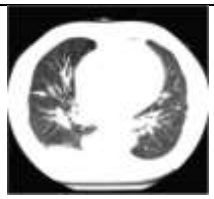
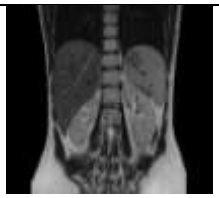
Image1	Image2	Image3	Image4	Watermark
				

Fig. 3. Medical images used in the proposed scheme

The two main evaluation parameters to describe performance of a watermarking scheme are fragility and imperceptibility. Fragility describes the resistance of the watermarking scheme against image manipulations due to attacks such as filtering, cropping, scaling, adding noise, and so on. The fragility is usually measured in terms of NCC and BER with respect to the original watermark and the extracted watermark in the presence of signal processing attacks. The imperceptivity of a watermarking scheme may be defined as measure of similarity between the original image and watermarked image. For evaluating this similarity, the parameter like the peak signal-to-noise ratio (PSNR) is used which may be defined as:

$$\text{PSNR(dB)} = \quad 10 \log \frac{(2^b - 1)^2}{MSE} \qquad (5)$$

Where 'b' refers to the number of bits used to represent the pixel intensity levels of an image. MSE, called mean squared error, is the average of the square of the difference between the two images $I$and $\hat{I}$of size M x N. If the pixels in error are few in number, then the value of the MSE returned is in the range of acceptable levels.

The quantitative metric that is commonly used at the extraction stage to evaluate the performance of the watermarking scheme is the Bit Error Rate (BER), which is calculated as follows:

$$BER\ (\%) = {}_{1/PQ}\left[\sum_{i=0}^{P-1}\sum_{j=0}^{Q-1} W(i,j) \oplus \widehat{W}(i,j)\right] \text{ x } 100 \qquad (7)$$

Where (i, j) gives the coordinates of a pixel such that W(m, n) and $\widehat{W}$ (i, j) are the pixel values of the original image and extracted image respectively at location (i, j). The value of BER should be as low as possible for a better watermarking scheme and if BER converges to zero then the original watermark is said to be completely recovered.Similarly, NCC is given mathematically as

$$NCC = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q} W(i,j)\hat{W}(i,j)}{\sum_{i=1}^{P}\sum_{j=1}^{Q}[W(i,j)]^2} \quad (8)$$

4.1 Imperceptivity Analysis

In this section the perceptual quality of the watermarked images has been analysed and presented. For evaluating the perceptual quality of the watermarked image the two quality metrics adopted in this work are SSIM and PSNR. The images of size 512 x 512 and watermark of size 32 x 32 has been used for analysing the proposed algorithm. The proposed scheme isanalysed for its performance using the medical general images as shown in Fig. 4.The proposed watermarking scheme attains an average PSNR value around >39dB when a 32 x 32 watermark logo is embedded in an image.

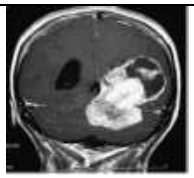
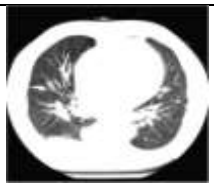
Watermarked Image				
PSNR (dB)	40.12	41.5	39.79	40.32
SSIM	0.99	0.99	0.99	0.99
Extracted Watermark				
BER (%)	0	0	0	0
NCC	1	1	1	1

Fig. 4. Watermarked images and extracted logos under no attack

4.2 Robustness Analysis

For the cases like privacy and copyright protection the robustness of a watermarking scheme is the most important factor. In this section the watermarked image is exposed to several attacks and the results hence recorded are analysed for robustness. NCC and BER are the two objective metrics which have been used for evaluation of the robustness of the proposed scheme. For the purpose of data privacy watermark has been embedded in a gray scale image or medical image. Fig. 5**,**shows the subjective and objective results obtained after different attacks on the watermarked image. The resulting watermarked image has been evaluated for performance against several attacks and the subjective and objective analysis has been done.

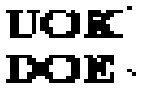
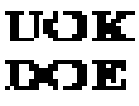
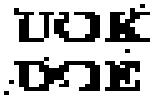
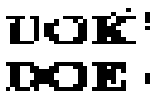
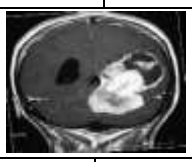
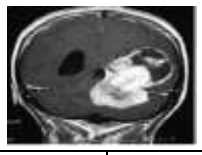
Attack Type	**No Attack**	**Histogram Equalization**	**JPEG 2000 (CR = 4)**	**Smoothing Filter**
Extracted Watermark				
NCC	1	0.9939	0.9874	0.9913
BER(%)	0	0.8789	1.7578	1.1719
Attack Type	**Rotation Recovery (45^{o})**	**Scaling Recovery (512-256-512)**	**JPEG (QF=20)**	**JPEG 2000 (CR = 8)**
Extracted Watermark				
NCC	0.9947	0.9987	0.9912	0.9987
BER(%)	1.0711	0.8789	1.4627	0.4833

Fig. 5. Extracted watermarks after different iterations and corresponding NCC and BER values

From the results it is clear that the proposed algorithm offers high visual quality and robustness and thus can be used for high quality medical image applications.

4.2.1 Rotation Recovery

In order to recover the watermark from the rotated image correctly a novel rotation recovery algorithm is applied. After detecting the angle of rotation using this algorithm the image is rotated back through that angle to get the correct image from which watermark can be obtained correctly. For obtaining the angle of rotation one has to know the dimensions of the original cover image first. The results obtained after rotation of watermarked image by various angles are shown in Fig. 6.

Rotation Attack	**Image1**				**Image2**			
	Rotation Attack		**Rotation Recovery**		**Rotation Attack**		**Rotation Recovery**	
	NCC	***BER***	***NCC***	***BER***	***NCC***	***BER***	***NCC***	***BER***
Rotate(5^{0})	0.62	37.12	0.991	1.87	0.63	37.65	0.993	1.76
								
Rotate(15^{0})	0.60	41.39	0.982	3.12	0.60	40.66	0.985	2.98
								
	0.58	43.22	0.976	4.83	0.57	43.01	0.978	4.05

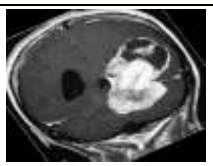
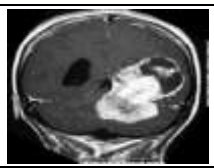
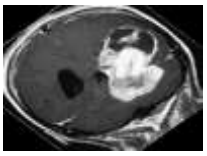
Rotate(30^0)								
	0.55	46.34	0.953	6.22	0.56	44.94	0.957	6.01
Rotate(44^0)								

Fig. 6. Watermarked images after ration attack of different degrees with NCC and BER values

5. CONCLUSION

In this article a robust watermarking technique has been proposed for securing medical information. In order to achieve the said goal a robust watermark is embedded in the host medical image. The experimental results prove that that the proposed system shows better robustnessagainst various signal processing attacks such as cropping, resizing, scaling, filtering and various other noise and compression attacks.The use of encryption ensures high level security of the sensitive medical information and can hence be used for all medical applications purposes. The use of the proposed technique in medical care will ensure the preservation of the privacy and data integrity of the patient information and hence a safer remote diagnosis can be done.

6. Acknowledgments

The authors would like to thank DeitY, Government of India, for supporting the proposed work under Visvesvaraya PhD Scheme and Department of Science and Technology (DST) New Delhi for supporting under DST inspire scheme.

REFERENCES

[1] A. C.Chozas, S.Memeti,& S.Pllana, (2017). Using Cognitive Computing for Learning Parallel Programming: An IBM Watson Solution. *Procedia Computer Science*, *108*, 2121-2130.

[2] S.Memeti& S.Pllana, (2018). PAPA: A Parallel Programming Assistant Powered by IBM Watson Cognitive Computing Technology. *Journal of Computational Science*.

[3] G.M. Bhat, M. Mustafa, S. Ahmad and J. Ahmad, VHDL modeling and simulation of data scrambler and descrambler for secure data communication, *Indian Journal of Science and Technology. 2009 Oct 1;2(10):*41-3.

[4] G.M. Bhat, M. Mustafa, S. A. Parah, J. Ahmad. Field programmable gate array (FPGA) implementation of novel complex PN-code-generator-based data scrambler and Descrambler. Maejo international journal of science and technology. 2010 Jan 1;4(1):125-35.

[5] S. Parah, J. Sheikh and G.M. Bhat, (2012a) 'On the realization of secure and efficient data hiding system using ISB and LSB technique', *Engineering E-Transaction, Malaysia, Vol. 7, No. 2*, pp.48–53, ISSN: 1823-6379.

[6] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2012b) 'On the realization of a secure, high capacity data embedding technique using joint top-down and down-top embedding approach', *Elixir Comp. Sci. &Engg.*, *Vol. 49*, pp.10141–10146.

[7] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2012c) 'Data hiding in ISB planes: a high capacity blind stenographic technique', in *Proc. of IEEE Sponsored Intl. Conference INCOSET-2012*, TiruchirapalliTamilnadu, India, pp.192–197.

[8] S. Parah, J. Sheikh and G.M. Bhat, (2013a) 'High capacity data embedding using joint intermediate significant bit and least significant technique', *International Journal of Information Engineering and Applications, Vol. 2, No. 11,* pp.1–11.

[9] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2013b) 'Data hiding in color images: a high capacity data hiding technique for covert communication', *Computer Engineering and Intelligent Systems, Vol. 4, No. 13,* pp.113–118.

[10] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2013c) 'On the realization of a spatial domain data hiding technique based on intermediate significant bit plane embedding (ISBPE) and post embedding pixel adjustment (PEPA)', *Proceedings of IEEE International Conference on Multimedia Signal Processing and Communication Technologies-IMPACT 2013, (AMU, Aligarh 23–25 November*) pp.51–55.

[11] S.A. Parah, J.A. Sheikh, A. M. Hafiz and G.M. Bhat, (2014a) 'Data hiding in scrambled images: a new double layer security data hiding technique', *Computers and Electrical Engineering, Vol. 40, No. 1*, pp.70–82, Elsevier.

[12] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2014b) 'A secure and efficient spatial domain data hiding technique based on pixel adjustment', *American Journal of Engineering and Technology Research*, US Library Congress, (USA), Vol. 14, No. 2, pp.38–44.

[13] S.A. Parah, J.A. Sheikh, A.M. Hafiz and G.M. Bhat, (2015a) 'A secure and robust information hiding technique for covert communication', *International Journal of Electronics*, Vol. 102, No. 8, pp.1253–1266, Taylor and Francis, UK.

[14] S.A. Parah, F. Ahad, J.A. Sheikh and G.M. Bhat, (2015b) 'On the realization of robust watermarking system for medical images', *12th IEEE India International Conference (INDICON) on Electronics, Energy, Environment, Communication, Computers, Control (E3-C3),* 17–20 December, JamiaMilliaIslamia, New Delhi, pp.1–6.

[15] S.A. Parah, J. A. Akhoon, J.A. Sheikh, N. A. Loan and G.M. Bhat, (2015c) 'A High capacity data hiding scheme based on edge detection and even-odd plane separation', *In India Conference (INDICON), 2015 Annual IEEE 2015 Dec 17 (pp. 1-5). IEEE.*

[16] S.A. Parah, J.A. Sheikh, F. Ahad, N. A. Loan and G.M. Bhat, (2015d) 'Information hiding in medical images: a robust medical image watermarking system for E-healthcare. *Multimedia Tools and Applications. 2017 Apr 1;76(8):10599-633.* Springer.

[17] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2015e) 'Hiding in encrypted images: a three tier security data hiding system', *Multidimensional Systems and Signal Processing*, September, Springer, DOI: 10.1007/s11045-015-0358-z.

[18] S.A. Parah, J.A. Sheikh, J.A. Akhoon, N. A. Loan and G.M. Bhat, Information hiding in edges: a high capacity information hiding technique using hybrid edge detection. *Multimedia Tools and Applications. 2018 Jan 1;77(1):185-207., Springer*, DOI: 10.1007/s11042-016-4253-x.

[19] S.A. Parah, J.A. Sheikh, N. A. Loan and G.M. Bhat, (2016b) 'Robust and blind watermarking technique in DCT domain using inter-block coefficient,' *Digital Signal Processing*, Elsevier, DOI: 10.1016/j.dsp.2016.02.005.

[20] S.A. Parah, F. Ahad, J.A. Sheikh, N.A. Loan and G.M. Bhat, (2016c) 'A New Reversible and high capacity data hiding technique for e-healthcare applications', M*ultimedia Tools and Applications*, Springer, DOI: 10.1007/s11042-016-4196-2.

[21] J.A. Sheikh, S.A. Parah and G.M. Bhat, (2016a) 'StegNmark: a joint stego-watermark approach for early tamper detection', *Intelligent Techniques in Signal Processing for Multimedia Security*, Vol. 660, Springer DOI: 10.1007/978-3-319-44790-2_17.

[22] J.A. Sheikh, S.A. Parah, U.I. Assad and G.M. Bhat, (2016b) 'Realization and robustness evaluation of a blind spatial domain watermarking technique', *International Journal of Electronics*, DOI: 10.1080/00207217.2016.1242162.

[23] F. Ahad, N. A. Loan, S. A. Parah, J.A. Sheikh and G.M. Bhat, (2016a) 'Pixel repetition technique: a high capacity and reversible data hiding method for e-healthcare applications', *Intelligent Techniques in Signal Processing for Multimedia Security*, Vol. 660, Springer, DOI: 10.1007/978-3-319-44790-2_17.

[24] N. A. Loan, S.A. Parah, J.A. Sheikh and G.M. Bhat, (2017) 'Utilizing neighbourhood coefficient correlation: a new image watermarking technique robust to singular and hybrid attacks', *Multidimentional Systems and Signal Processing*, DOI: 10.1007/s11045-017-0490-z.

[25] F. Ahad, S.A. Parah, J.A. Sheikh and G.M. Bhat, (2017) 'Hiding clinical information in medical images: a new high capacity and reversible data hiding technique', *Journal of Biomedical Informatics*, February, Vol. 66, pp.214–230 [online] DOI: http://dx.doi.org/10.1016/j.jbi.2017.01.006 (accessed 21 September 2017).

[26] Das C, Panigrahi S, Sharma VK., Mahapatra KK (2014) A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. *Int. J. Electron. Commun. (AEÜ) 68:* 244– 253.

[27] N. A. Loan, S.A. Parah, J.A. Sheikh and G.M. Bhat, (2016b) 'A robust and computationally efficient digital watermarking technique using inter block pixel differencing', *Multimedia Forensics and Security*, Vol. 115, Springer DOI: 10.1007/978-3-319-44270-9_10.

[28] Roy, S. and Pal, A.K., 2017. A blind DCT based color watermarking algorithm for embedding multiple watermarks. *AEU-International Journal of Electronics and Communications*, *72*, pp.149-161.

[29] Abhilasha Sharma, Amit Kumar Singh and S P Ghrera, Sharma, Secure Hybrid Robust Watermarking Technique for Medical Images. *Procedia Computer Science 70 (2015),* 778 – 784.

[30] Verma, V.S., Jha, R.K. and Ojha, A., 2015. Significant region based robust watermarking scheme in lifting wavelet transform domain. *Expert Systems with Applications*, *42*(21), pp.8184-8197.

[31] Guo J, Zheng P, Huang J (2015) Secure Watermarking Scheme against Watermark Attacks in the Encrypted Domain. *J. Vis. Commun. Image R, 00*:1–3.

[32] Ma F, Zhang JP,Zhang W (2012), A Blind Watermarking Technology Based on DCT Domain, *International Conference on Computer Science and Service System*: 398-401.

[33] Chen, J.X., Zhu, Z.L., Fu, C., Zhang, L.B. and Zhang, Y., An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach. *Communications in Nonlinear Science and Numerical Simulation, 23(1),2015,* 294-310.

[34] Kanso, A., and M. Ghebleh. An efficient and robust image encryption scheme for medical applications. *Communications in Nonlinear Science and Numerical Simulation, vol. 24, no. 1, 2015*, pp. 98-116.