

An Innovative Approach to Solve Healthcare Issues Using Big Data Image Analytics

Ramesh R., Kalaignarkaranidhi Institute of Technology, Coimbatore, India

Udayakumar E., Kalaignarkaranidhi Institute of Technology, Coimbatore, India

Srihari K., SNS College of Engineering, Coimbatore, India

Sunil Pathak P., Amity School of Engineering and Technology, Amity University, Noida, India

ABSTRACT

The increasing adoption of transmission of medical images through internet in healthcare has led to several security threats to patient medical information. Permitting quiet data to be in peril may prompt hopeless harm, ethically and truly to the patient. Accordingly, it is important to take measures to forestall illicit access and altering of clinical pictures. This requests reception of security components to guarantee three fundamental security administrations – classification, content-based legitimacy, and trustworthiness of clinical pictures traded in telemedicine applications. Right now, inside created symmetric key cryptographic capacities are utilized. Pictorial model-based perceptual image hash is used to provide content-based authentication for malicious tampering detection and localization. The presentation of the projected algorithm has been evaluated using performance metrics such as PSNR, normalized correlation, entropy, and histogram analysis, and the simulation results show that the security services have been achieved effectively.

KEYWORDS

AES-GCM, Big Data, Content-Based Authenticity, ECDSA, Healthcare, Image Processing, Medical Diagnosis, Perceptual Image Hash, Tampering Detection, Tampering Localization, Whirlpool Hashing

1. INTRODUCTION

Telemedicine is a medicinal consideration practice which gives various advantages, Along these lines, there is a prompt requirement for verified plans for safe trade of DICOM pictures and information which decreases the plausibility of hacking. The systems to accomplish three significant telemedicine security administrations: secrecy, legitimacy and honesty. Content based confirmation is expected to distinguish and find the altered districts in a DICOM picture. Implanting and corrupting the medicinal picture, may actuate serious protection from its reception by therapeutic principles. In this paper, a crypto-based calculation is proposed which is fit for giving classification, content based realness and trustworthiness of DICOM pictures.

DOI: 10.4018/IJBDAH.20210101.oa2

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

2. RELATED WORKS

Many threats posed by DICOM images. Some of those algorithms and their drawbacks are described in the next sections.

2.1. Crypto-Based Algorithms

This may reliably get modified. Believability and uprightness are suited the pixel data using propelled marks with inside delivered keys and it fails to give content based validity which is basic for change restriction. The count furthermore doesn't give mystery, validity and decency for the header data using big data.

Owing to the limitations referred to above, Al-Haj (Al-Haj & Hussein, 2015) propose a novel arrangement that keeps an eye on the security issues looked by the above arrangement. The count gives authenticity, protection and decency. In any case, the estimation doesn't have the modify constraint limit which is needed in the dependability affirmation of restorative pictures.

2.2. Hybrid Algorithms

At the point when everything is said in done, give uprightness restorative picture, while CRCs are fittingly used perceive modified zones in the got picture. Nevertheless, crossbreed estimations experience from being computation raised. Likewise, 1piece change in a cyclic redundancy code or a hash code will provoke fake affirmation and wrong genuineness check.

3. PROPOSED ALGORITHM

The proposed calculation tends to every one of the restrictions looked by earlier works referenced in Section 2 by giving privacy. It likewise gives content based validation to the pixel information of DICOM picture by utilizing visual model based perceptual picture hashing capacity for altering recognition and limitation.

The proposed calculation comprises of two systems: the encryption and mark creation methodology, the decoding and mark check technique and the alter confinement strategy if the mark is seen as inauthentic. The calculation utilizes AES-GCM, the whirlpool hash capacity and ECDSA for DICOM header information and AES-GCM, the perceptual picture hashing and ECDSA for DICOM pixel information which gives classification, uprightness and substance based validness for the DICOM pictures.

3.1. Encryption and Signature Creation Procedure

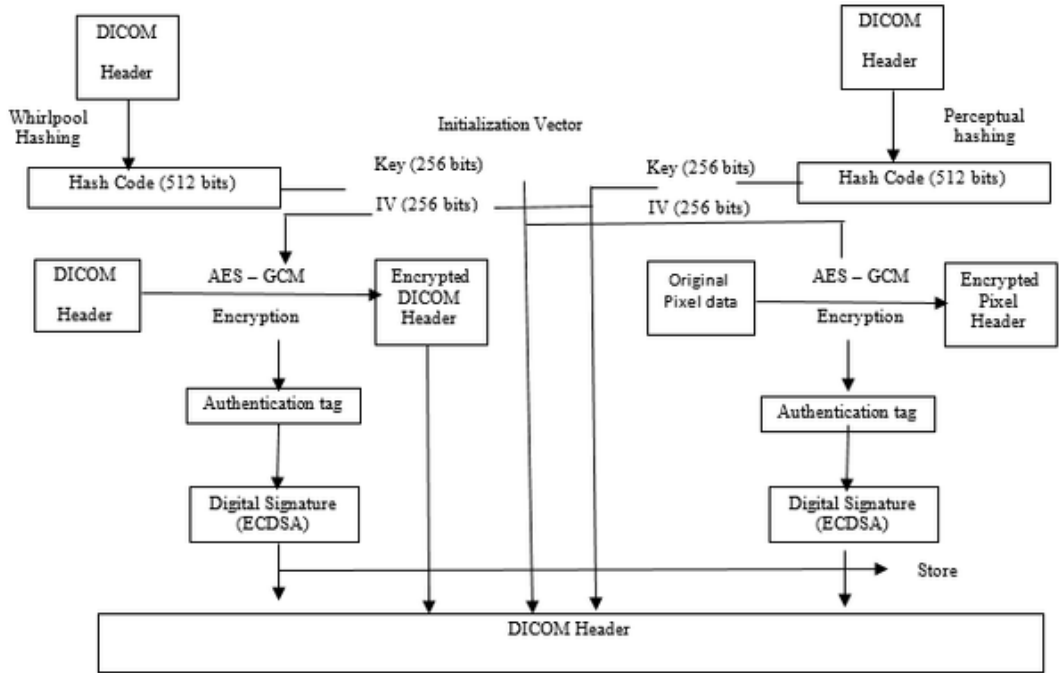
A strategy has the classified characteristics of header information and pixel information sources of info and its yields are halfway scrambled DICOM header and completely encoded pixel information. The system is appeared in Figure 1.

3.1.1. Header Data Confidentiality

A strategy scrutinizes each and every private nature of the header data and scrambles their novel characteristics using AES-GCM using big data. The customer won't have the choice qualities, the instatement vector and the encryption key vary beginning with one picture then onto the following. This sidesteps the potential weakness introduced in the encryption platform (Santhi, 2017b). This strategy decodes the encoded pixel information and the halfway scrambled DICOM header information, and confirms their validness (Das & Kundu, 2013) and honesty as appeared in Figure 2 and Figure 3. On the off chance that the pixel information is seen as inauthentic, at that point the strategy will find the altered locale in the DICOM picture (Vetrivelan, 2017).

The names, validness and decency (Mohan, 2020; Ramesh, 2016) of the arranged characteristics of the pixel data are affirmed. If the two marks are not composed, by then adjusting control estimation

Figure 1. Encryption and signature creation producer of the proposed algorithm



as delineated in zone IV and as showed up in Figure 3. Must be applied and the modified areas must be found (Santhi, 2017a).

4. CRYPTOGRAPHIC FUNCTIONS USED IN THE PROPOSED ALGORIHTM

The cryptographic capacities that are utilized in the proposed calculation and their determination criteria are portrayed in this segment.

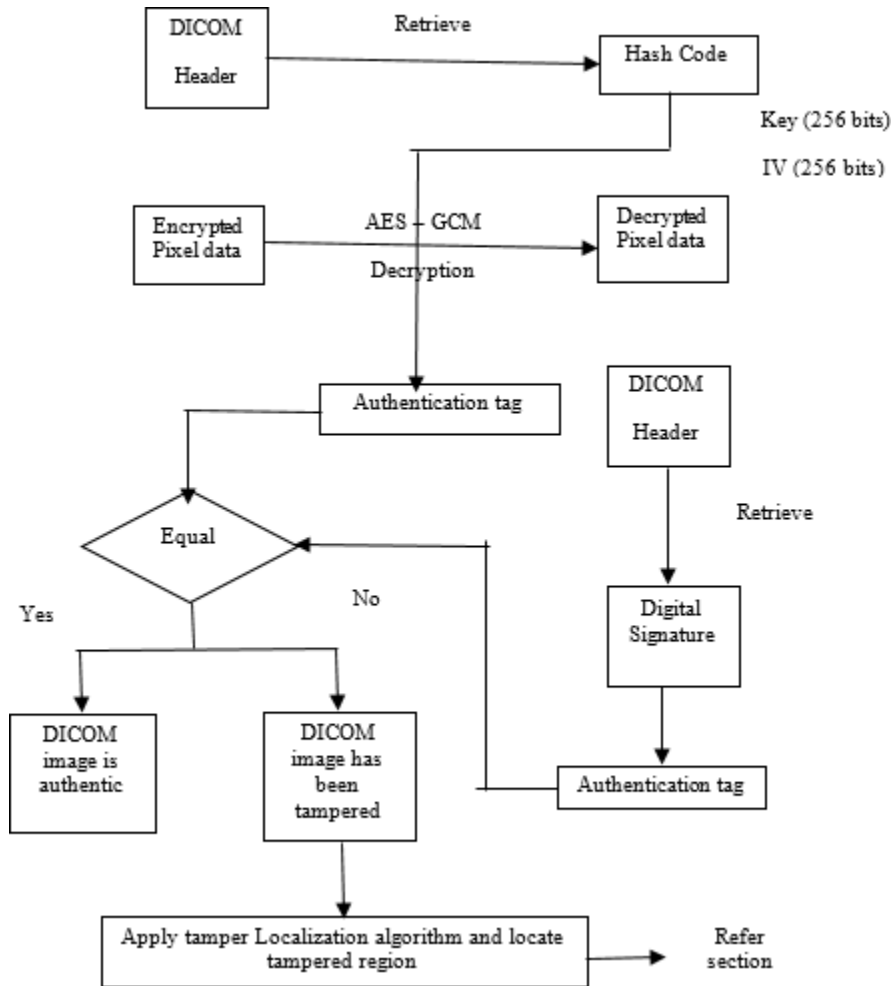
4.1. Perceptual Image Hashing

Perceptual picture hashing picture content verification using big data. Figure 4: Flow chart for hash generation algorithm. The perceptual picture hashing plan (Wang et al., 2015) incorporates a hash age calculation, an altering discovery calculation and an altering limitation algorithm. 1) Hash age calculation: The hash age calculation comprises of two phases (Zhou et al., 2017) include extraction and pressure and coding. The procedure is appeared in Figure 4. a) Perceptual (Dr, 2017) Feature extraction.

4.2. Perceptual Feature Extraction

1. **Key-Point-Based Features:** The key-point-based features for the input DICOM image are extracted using SIFT feature extraction algorithm (Lowe, 2004).
2. **Block-Based Features:** The block features for the input DICOM image are extracted by taking DCT.
3. **Compression and Projection:** These have projection of the extracted image features. The result obtained is combined to form an intermediate hash code (Al-Haj & Abdel-Nabi, 2017) (Figure 5).

Figure 2. Pixel data decryption and signature verification procedure



4.3. Compression and Coding

The algorithm process is as follows:

Stage 1: Huffman translating and unscrambling is applied to the recovered perceptual hash from the DICOM header to get transitional hash of the first picture.

Stage 2: For got picture, an addition activity is applied to get a similar size with unique picture. At that point SIFT highlights are removed. At that point, 1-level db1 wavelet change is applied to the element focuses set.

Stage 3: To endure geometric contortions, it is important to coordinate the component point sets of both unique and got picture content. By applying the SIFT coordinating calculation (Lowe, 2004), n sets of most-comparative element focuses can be gotten. At that Point, the component point sets are refreshed as coordinated element focuses. A relative change network π are assessed (Kim, 2019).

Stage 4: The came about picture is separated into non-covering $P \times (P=8)$ squares. DCT is applied to each square. From that point onward, apply the Gaussian arbitrary grid. The moderate hash is acquired. Utilizing the Huffman coding, a last hash code of the got picture can be produced.

Figure 3. Header data decryption and signature verification procedure

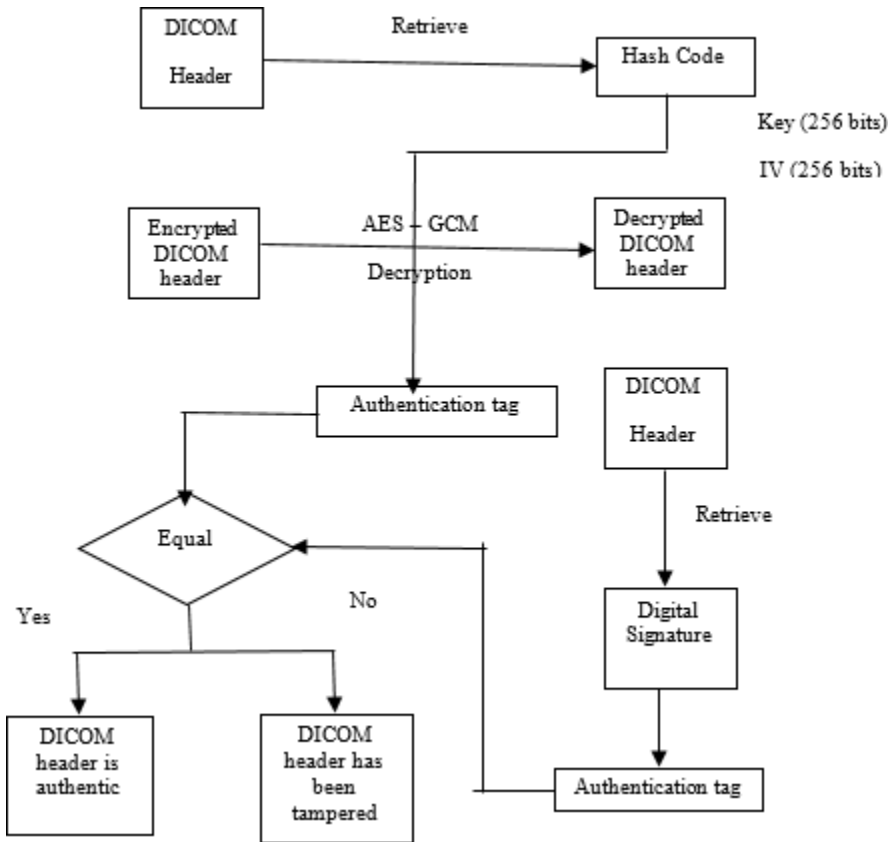
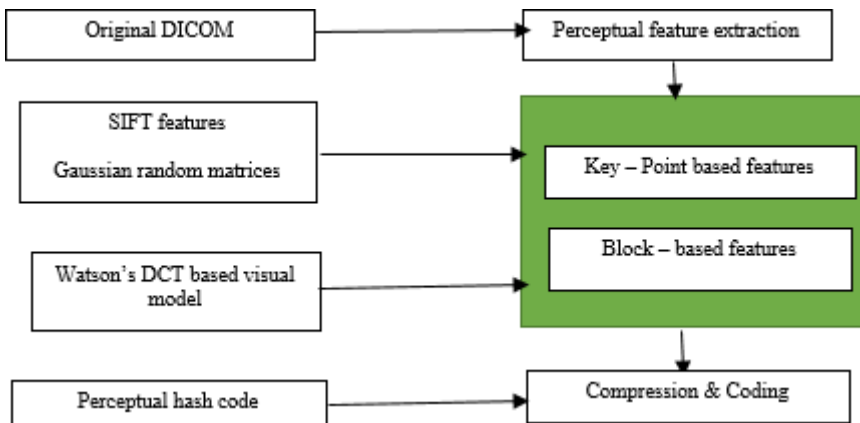
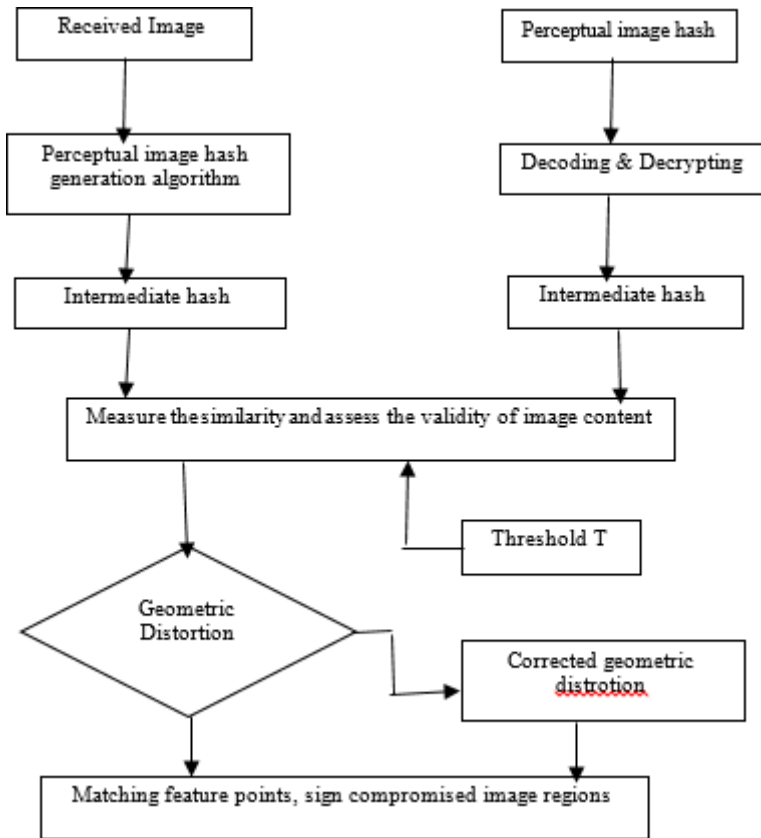


Figure 4. Flow chart for hash generation algorithm



Stage 5: To gauge the comparability between pictures hinders in unique picture and picture obstructs in got picture, the Euclidean separation D between them is assessed (Yogadinesh, 2015).

Figure 5. Schematic diagram of tampering detection and location



Stage 6: If $D > T$, at that point the tried picture ought to be viewed as inauthentic; go to stage 7, else the tried picture ought to be viewed as legitimate, where T is a limit.

Stage 7: The Euclidean separation D_a between each pair of coordinated element focuses in sets acquired from unique and got pictures are evaluated.

If $D_a > T_a$, the tested image should have undergone geometric transformation (Zhou et al., 2015).
 If $D_a \leq T_a$, the tested image should not be considered undergoing geometric transformation.

5. PERFORMANCE ANALYSIS

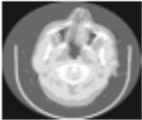
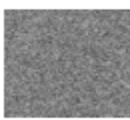
The exhibition calculation with respect to the accomplishments necessities has been assessed by considering a benchmark set of 5 CT DICOM cerebrum pictures and a CR DICOM hand picture. The calculation was actualized utilizing MATLAB 2015a. If the encoded picture is exceptionally uncorrelated to the first plain picture, at that point the secrecy is guaranteed. To gauge the relationship between the plain and encoded pictures created by the proposed calculation, likeness investigation, entropy examination and histogram investigation has been led. Time examination has additionally been directed to assess the computational necessities of the proposed calculation. The alter discovery and confinement results are appeared in Figure 9.

5.1. Similarity Analysis

Similarity analysis is a display metric used to check the degree of comparability between two automated pictures. If the plain and the figure pictures are absolutely uncommon. The PSNR regard got by the proposed estimation is showed up in Figure 6. The low PSNR regard exhibit that the two pictures are uncorrelated.

The entropy esteem got for the proposed calculation is appeared in Figure 7, whose worth is which exhibit the viability proposed calculation sequestered from everything the subtleties of the first picture (Yogeshwaran, 2019).

Figure 6. Correlation and PSNR values between the plain and cipher images

Original image	Cipher image	Correlation Factor	PSNR (db)
		0.0086	11.2875

5.2. Histogram Analysis

See Figure 8.

5.3. Time Analysis

The complete decoding time the proposed calculation have been estimated and seen as 925.6s and 987.4s separately (Ramesh, 2018). The proposed calculation invest the vast majority of their energy in executing the AES-GCM encryption and unscrambling using big data techniques.

5.4. Performance Comparison

The proposed algorithm has been related with the Al-Haj’s algorithm (Al-Haj, 2015) which is shown in Table 1. Comparison is normalized correlation, PSNR and entropy.

Figure 7. Entropy values for the plain and cipher images

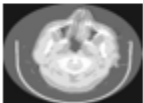
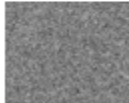
Original image	Entropy of original image, bits/pixel	Cipher image	Entropy of cipher image, bits/pixel
	5.5719		7.8180

Figure 8. Plain and cipher images and corresponding histograms

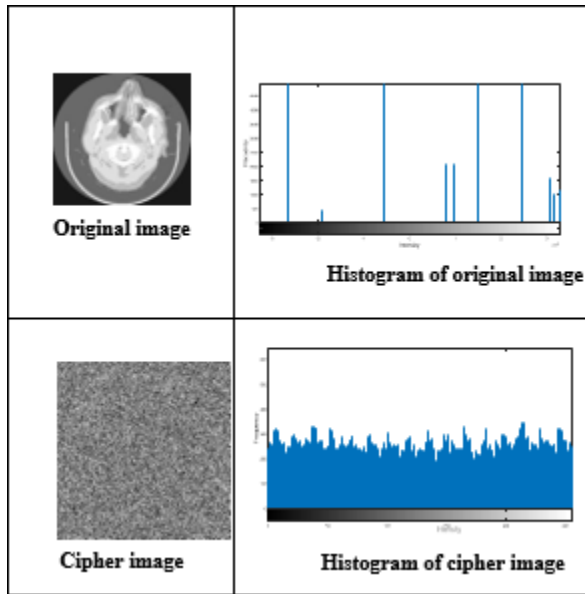
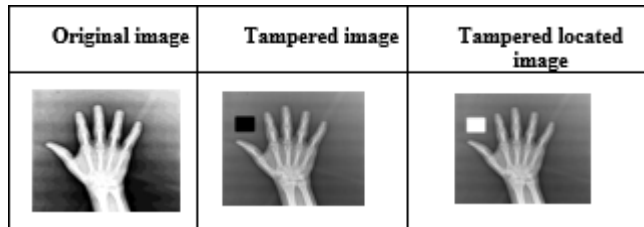


Figure 9. Tampering localization result



6. CONCLUSION

The proposed calculation gives classification, genuineness and uprightness for both the header information and pixel information. Notwithstanding that, it gives content-based legitimacy to the pixel information for altering identification and restriction. Altering restriction is a helpful usefulness since trustworthiness control dependent on the specific protection of all pieces of the picture might be superfluously severe as contortions on the picture may likewise be because of commotion beginning

Table 1. Comparison with Al-Haj's Algorithm

Parameters	Proposed Algorithm	Al-Haj's Algorithm (Al-Haj & Hussein, 2015)
Normalized correlation	0.0086	0.0081
PSNR (dB)	11.2875	11.1309
Entropy, bits/pixel	7.8180	7.8909

from the transmission procedure. Giving security administrations to the header information is significant since it contains the classified information which ought to be ensured.

For the future, this proposed calculation will be executed in equipment and execution will be broke down progressively utilizing Wireless access explore fringe (WARP) V3 board which is utilized essentially in remote transmission applications.

REFERENCES

- Al-Haj, A. (2015). Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. *Journal of Digital Imaging*, 28(2), 179–187. doi:10.1007/s10278-014-9734-8 PMID:25266442
- Al-Haj & Abdel-Nabi. (2017). Digital image security based on data hiding and cryptography. *2017 3rd International Conference on Information Management (ICIM)*.
- Al-Haj, G. A., & Hussein, N. (2015). Crypto-based algorithms for secured medical image transmission. *IET Information Security*, 9(6), 365–373. doi:10.1049/iet-ifs.2014.0245
- Das, S., & Kundu, M. K. (2013). Effective management of medical information through ROI-lossless fragile image watermarking technique. *Computer Methods and Programs in Biomedicine*, 111(3), 662–675. doi:10.1016/j.cmpb.2013.05.027 PMID:23816251
- Dr, P. (2017). An Identification of efficient vessel feature for Endoscopic Analysis. *Research Journal of Pharmacy and Technology*, 10(8), 2633–2636. doi:10.5958/0974-360X.2017.00467.X
- Kim, K.S. (2019). Region-based tampering detection and recovery using homogeneity analysis in quality-sensitive imaging. *Computer Vision and Image Understanding*.
- Lowe, D. G. (2004). Distinctive image features from scale-invariant key points. *International Journal of Computer Vision*, 60(2), 91–110. doi:10.1023/B:VISI.0000029664.99615.94
- Mohan, N. (2020). Classification of Malignant Melanoma and Benign Lung Cancer by using Deep Learning Based Neural Network. *International Journal of Innovative Technology and Exploring Engineering*, 9(3).
- Ramesh. (2018). A Review on diagnosis of Malignant Melanoma from Benign Lesion by using BPNN and ABCD Rule Parameters. *International Research Journal of Pharmacy*, 9(10).
- Ramesh, C. (2016, December). Region Growing Image Segmentation for Newborn Brain MRI. *BioTechnology: An Indian Journal*, 12(12), 1–8.
- Santhi. (2017a). Automatic Detection of Diabetic Retinopathy through Optic Disc using Morphological Methods. *Asian Journal of Pharmaceutical and Clinical Research*, 10, 28-31.
- Santhi, S. (2017b). An Unified Reeb Analysis for Cortical Surface Reconstruction of MRI Images. *Biomedical & Pharmacology Journal*, 10(02), 939–945. doi:10.13005/bpj/1188
- Vetrivelan, . (2017, May). TB screening using SVM and CBC techniques. *Current Pediatric Research, Allied Academies*, 21(2), 338–342.
- Wang, X., Pang, K., Zhou, X., Zhou, Y., Li, L., & Xue, J. (2015). A visual model-based perceptual image hash for content authentication. *IEEE Transactions on Information Forensics and Security*, 10(7), 1336–1349. doi:10.1109/TIFS.2015.2407698
- Yogadinesh, S. (2015). Certain Investigation of Identify the New Rules and Accuracy using SVM algorithm. *Middle-East Journal of Scientific Research*, 23, 2074–2080.
- Yogeshwaran, K. (2019). An Efficient Tissue Segmentation of Neonatal Brain Magnetic Resonance Imaging. *Research Journal of Pharmacy and Technology*, 12(6), 2963–2966. doi:10.5958/0974-360X.2019.00499.2
- Zhou, G., Xiao, L., Pei, X., Li, C., Qin, H., Zhang, J., & Fang, Z. (2017). Paper infrared image retrieval of power equipment based on perceptual hash and SURF. *2017 9th International Conference on Advanced Infocomm Technology (ICAIT)*. doi:10.1109/ICAIT.2017.8388951
- Zhou, Y., Li, L., & Xue, J. (2015). A Visual Model- Based Perceptual Image Hash for Content Authentication. *IEEE Transactions on Information Forensics and Security*.

R. Ramesh is working in Department of Electronic and Communication Engineering from KIT- Kalaigarkaranidhi Institute of Technology, Coimbatore. I had complete my BE in Electronics and Communications Engineering from Anna University Regional Center, Coimbatore and ME from Dr. Mahalingam College of Engineering and Technology, Pollachi. His research areas include Antennas design and Microwave Engineering.

E. Udayakumar is working as Assistant Professor in Department of Electronics and Communication Engineering at KIT-Kalaigarkaranidhi Institute of Technology, Coimbatore, Tamilnadu India. He completed his Master degree (Communication Systems) from Sri Ramakrishna Institute of Technology, Coimbatore in the year 2015. He had published 20 Papers in International Journals, 20 papers in National & International Conferences. He had authored three books on Image processing and VLSI. He is a Life Member in various Professional Societies like IETE, ISTE, IEI, SSI, BMESI, IAENG. His Research Interests includes Medical Image Processing, Wireless Communication and Antennas.

K. Srihari received the M.E. and Ph.D. degree from Anna University, Chennai. He is currently working as an Associate Professor in the Department of Computer Science and Engineering, SNS College of Engineering, affiliated to Anna University- Chennai, Tamilnadu, India. Dr. K. Srihari have published over 60 papers in international journals and his research area includes Information and Communication engineering.

Sunil Pathak received the M. Tech degree in Information Technology from Tezpur Central University, Tezpur, Assam, India in 2006. He has completed his Ph.D. from JK Lakshmi Pat University, Jaipur, India in Mobile Ad-Hoc Network. He is currently working as an Associate Professor & Head, in the Department of Computer Science & Engineering in Amity University. He has 13 Years of teaching experience. His area of interest includes Routing Protocol, Security, and Power Constraints in Mobile Ad-Hoc Network, Computer Networks and Programming Languages.