iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VIII **Month of publication:** August 2020

DOI: https://doi.org/10.22214/ijraset.2020.30857

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

An Efficient Method for Secure Access of EHR

Sowmyashree A N[1], Sahanaraj B S[2]
[1]*Mtech Student,* [2]*Assistant Professor, Department of Electronics and Communication, PES College of Engineering, Mandya, Karnataka, India*

Abstract: ***Healthcare systems is preservation of patients knowledge against the potential contender. It is essential to own certain data access mechanisms that ensures approved entities can access the patients medical documentation. The Electronic Health Records (EHR) possess the patient`s medical details and their health history. Electronic health record will improve quality care by using the data and analytics to prevent hospitalizations among risky patients. The health records draw the attention of the attackers because it preserves key data. Now a days, healthcare data are often generated, reproduce and alter quicker than ever before. We developed to ensure the security by means of proper encryption and decryption in the Electronic Health Record in the Healthcare System. The proposed algorithm uses Discrete Cosine Transform (DCT) for image transformation(that is to change the pixel position with less memory).***

Keywords: Electronic Health Record(EHR);Security.

I. INTRODUCTION

In hospitals the defence of the patients data from various stakeholders. Its essential to secured the patients database. That can be verify only the permitted person can entry the patients data. These days, health care data can be generated, replicated and changed quicker than ever before. EHR not only provide several helpful information for diagnosis and scientific research but also it offers one type of judgement basis for controlling medical discussion. So, it has attracted a wide scope of awareness as well as the government, the medical groups, cybersecurity branch, etc. since the medical data is critical for the diagnosis and it is private and careful for patients. Thus, data allocating and privacy protection issues are crucial in EHR. The medical data should be stored, handled and obtained securely. In particularly, the doctor generally demands to know the medical history of the patient when she or he creates the diagnosis or treatment. However, the patient cannot be essentially related his or her medical background, which will trobles the latest treatment. Thus, in EHR, historical medical data caused by different doctors in different hospitals should be effective of being securely and timely queried by a authorized with the patient`s authorization.

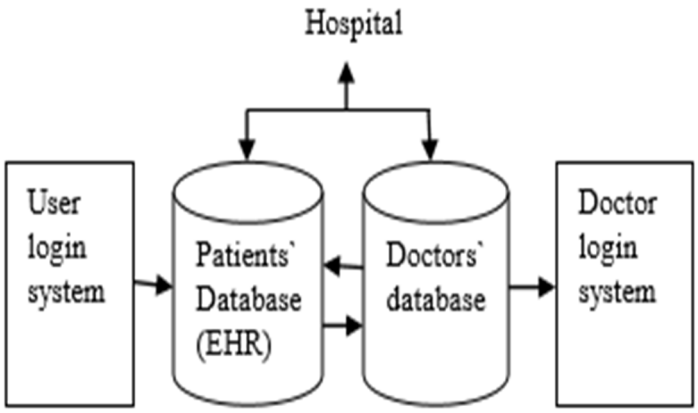


Figure 1: A simplified E-healthcare systems.

Figure 1 shows the interaction between the patients` database and doctors` data base and its simple to access patient database. The user login system as user-name and password. Within the doctors` login system produce valid doctors in that hospital. Patient's database` contains patients name, date of birth, email, address and EHR file. EHR (electronic health record) is a patient records that keeps electronically in a digital format. EHR`s contains doctor name, patients demographics, billing information, progress notes, insurance, laboratory data, pharmacy. EHR`s are actually patient – centred records, they make details available instantly, " whenever and where ever it is needed".

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

II. RELATED WORK

The aim specified in [6] is to design cloud-assisted PHR secure sharing system. It provides fine-grained access control, confidentiality, authenticity and sender privacy of PHR data. Hence, a large number of pairing and modular elaboration computations bring more and more computational overhead during designcryption process. In this scheme, the heavy computations are outsourced to ciphertext transformed server(CTS), only leaving a small computational overhead for the PHR user. At the same time , the extra communication overhead in our scheme is actually tolerable. In order to synthesize the conflict of high computational overhead and low efficiency in the designcryption process, an outsourcing methods is proposed in this paper.
The main focus of [8] is about Collaborative healthcare environment provide potential profits as well as enhancing the health care quality delivered to patients and lowering costs. As a direct consequence, sharing of electronic health records (EHRs) among health care providers has experienced a noteworthy growth in the last years, since it enables physicians to remotely monitor patients' health and enables individuals to handle their own health data more easily. However, these scenarios face significant challenges concern with security and privacy of the especially sensitive information holds in EHRs. Thus, a flexible, efficient and standards-based solution is indispensable to guarantee selective identity information disclosure and preserve patient`s privacy.

III. METHODOLOGY

Image encryption techniques try to convert original image to another image that is hard to understand to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. electronic health record is taken as image ,that image is implemented to the process of encryption and decryption method using substitution and DCT.

A. Block Diagram of Encryption

The steps required for encryption of image is shown below.

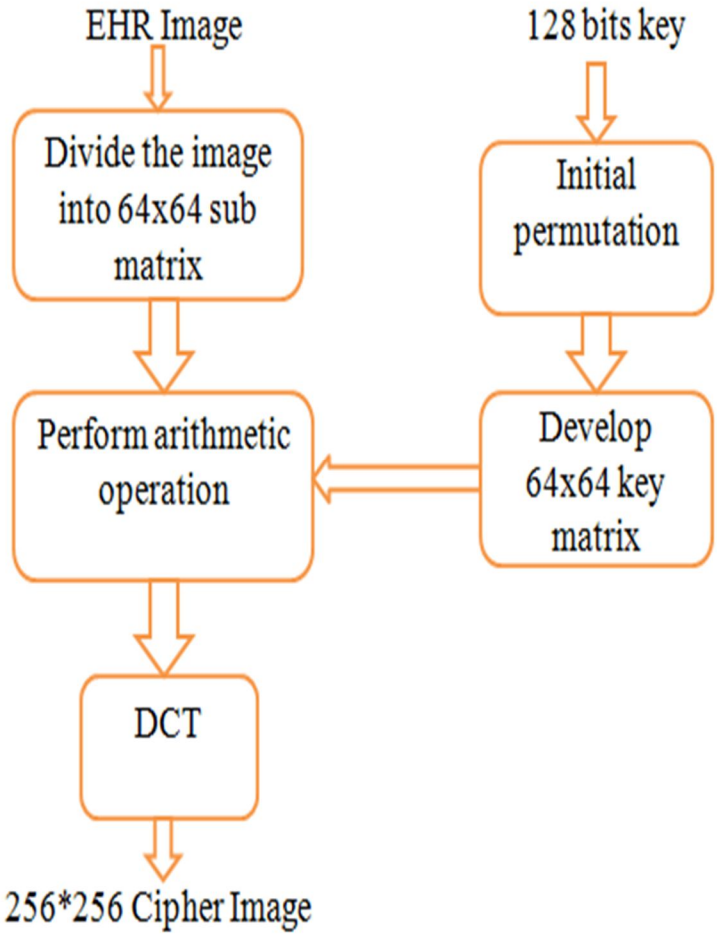


Figure 2: Block diagram of encryption process

The above figure shows the block diagram shows the block diagram of encryption, to encrypt the image first read the grayscale image and convert it into suitable form, which can be in any MATLAB format with any resolution (ex:256x256,1080x1080,570x320, etc) and permutation is performed on 128bit key to develop 64x64 sub matrixes. Arithmetic operation is performed with the divided 64x64 sub matrixes, these steps are repeated up to 16 blocks. Finally discrete cosine transform(DCT) is applied to entire image to obtain cipher image, the following each steps describe the process of image encryption.

1) Read The Image
2) Divide The Image
3) Generate Secret Key
4) Initial Permutation And Develop Matrix
5) Logical Operation
6) Discrete Cosine Transform(DCT)

B. Block Diagram of Decryption

To decrypted the encrypted image following steps are followed.

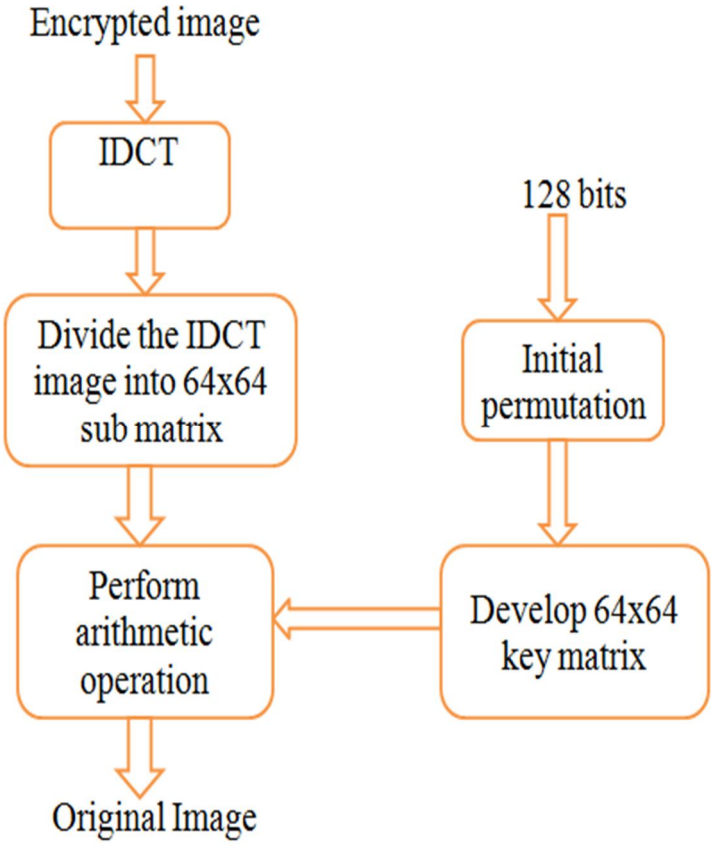


Figure 3: Block diagram of decryption process

For decrypting the cipher image the reverse process of encryption is performed, in which the inverse discrete cosine transform is taken for encrypted image and 128 bit key divided 64x64 IDCT image, this steps is repeated up to 16 blocks to obtain original image. The following each steps describe the decryption process.

1) Cipher Image.
2) Inverse Discrete Cosine Transform(IDCT).
3) Dividing The IDCT Image.
4) Logical Operation In IDCT.

IV. RESULT AND DISCUSSION

The proposed system is implemented successfully and the following results are obtained.

A. Implementation Results in MATLAB

1) Electronic Health Record Image 1: The following results show the original image 1, encrypted image 1, decrypted image 1, with its equivalent histogram images. Figure 4 its show the original image and equivalent histogram image. In the histogram, the X-axis the Y-axis shows the frequency of these intensities.

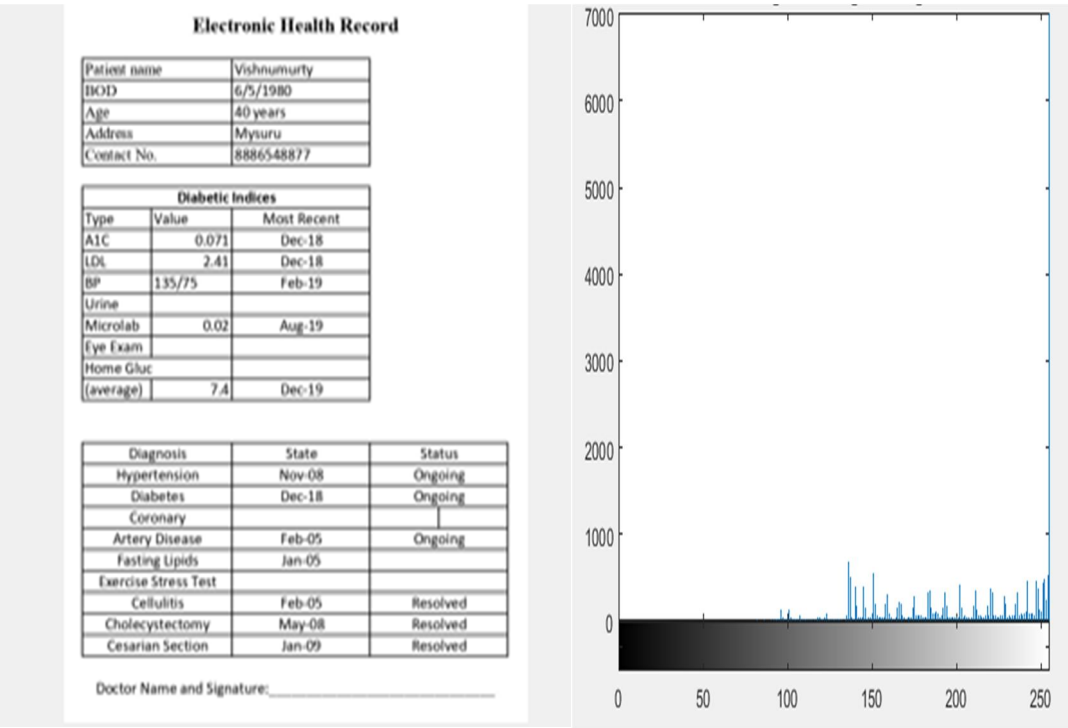


Figure 4: The Original EHR Image 1 And Its Equivalent Histogram Image.

Figure 5 shows the encrypted image with equivalent histogram. In the histogram, the X-axis shows the gray level intensities and Y-axis shows the frequency of these intensities. The histogram of encrypted image shows the nullified line(no information).

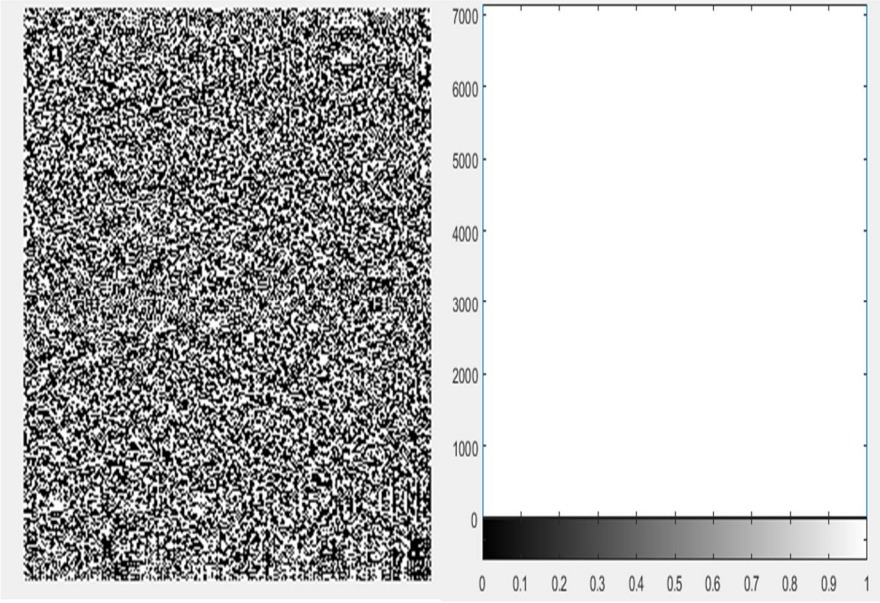


Figure 5: The Encrypted EHR Image 1 And Its Equivalent Histogram Image.

Figure 6 shows the decrypted image and equivalent histogram image. In the histogram, the X-axis shows the gray level intensities and the Y-axis shows the frequency of these intensities.

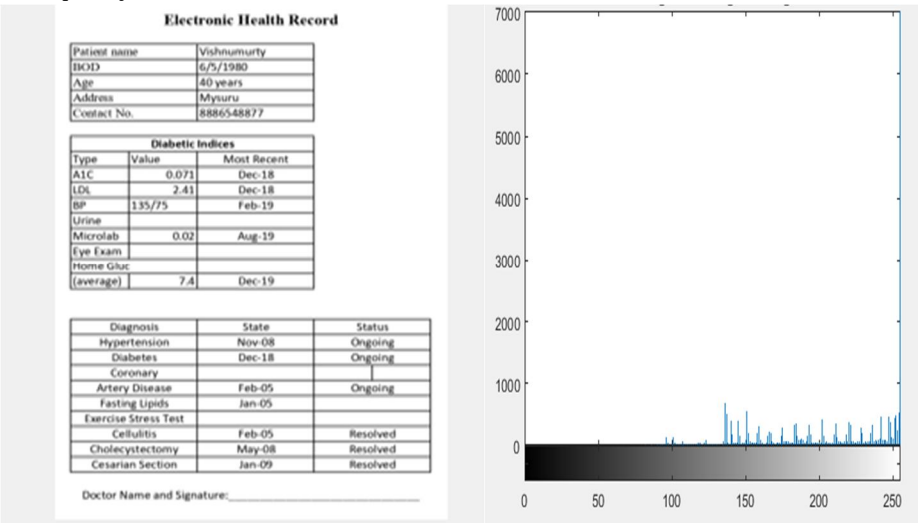


Figure 6: The Decrypted Image 1 And Its Equivalent Histogram Image.

2) Electronic Health Record 2: The following results show the original image 2, encrypted image 2, decrypted image 2 with its equivalent histogram images.

Figure 7 its shows the original image and equivalent histogram image. In the histogram, the X-axis shows the gray level intensities and Y-axis shows the frequency of these intensities.

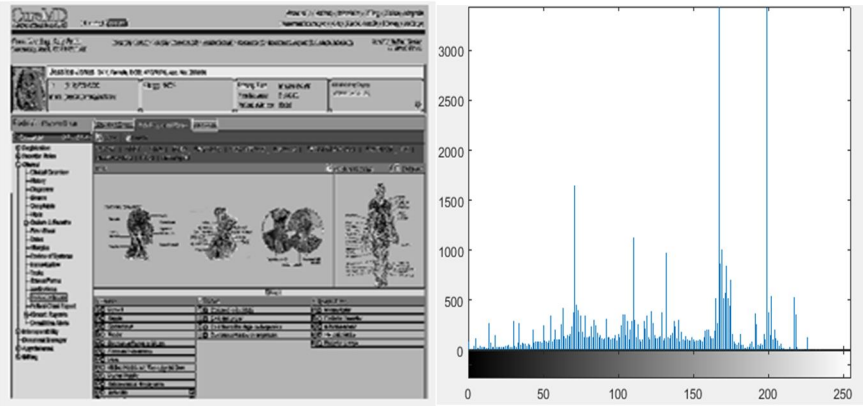


Figure 7: The original EHR image 2 and its Equivalent histogram image.

Figure 8 shows the encrypted image with equivalent histogram. In the histogram, the X-axis shows the gray level intensities and the Y-axis shows the frequency of these intensities. the histogram of encrypted image shows the nullified line(no information).

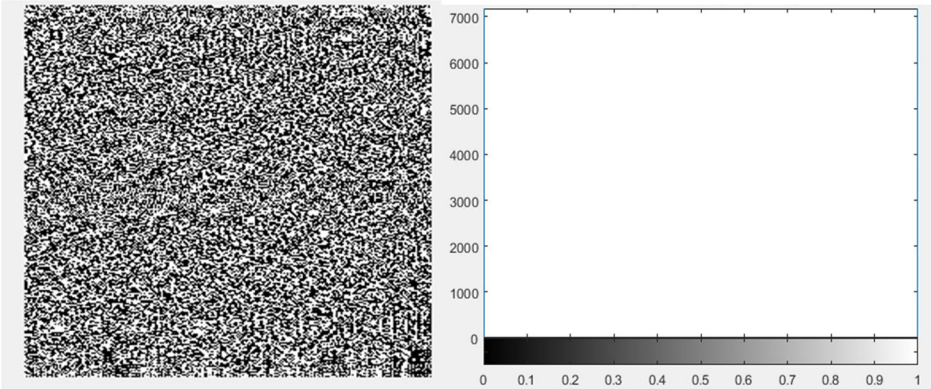


Figure 8: The Encrypted EHR Image 2 And Its Equivalent Histogram Image.

Figure 9 shows the decrypted image and equivalent histogram image. In the histogram, the X-axis shows the gray level intensities and the Y-axis shows the frequency of these intensities.

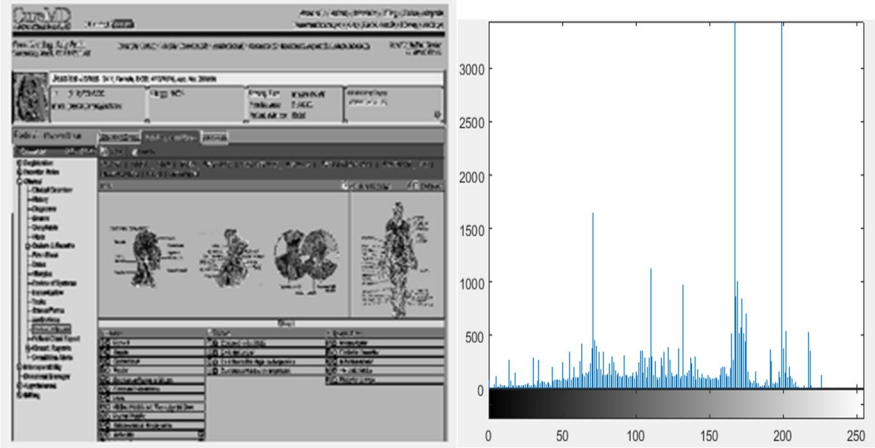


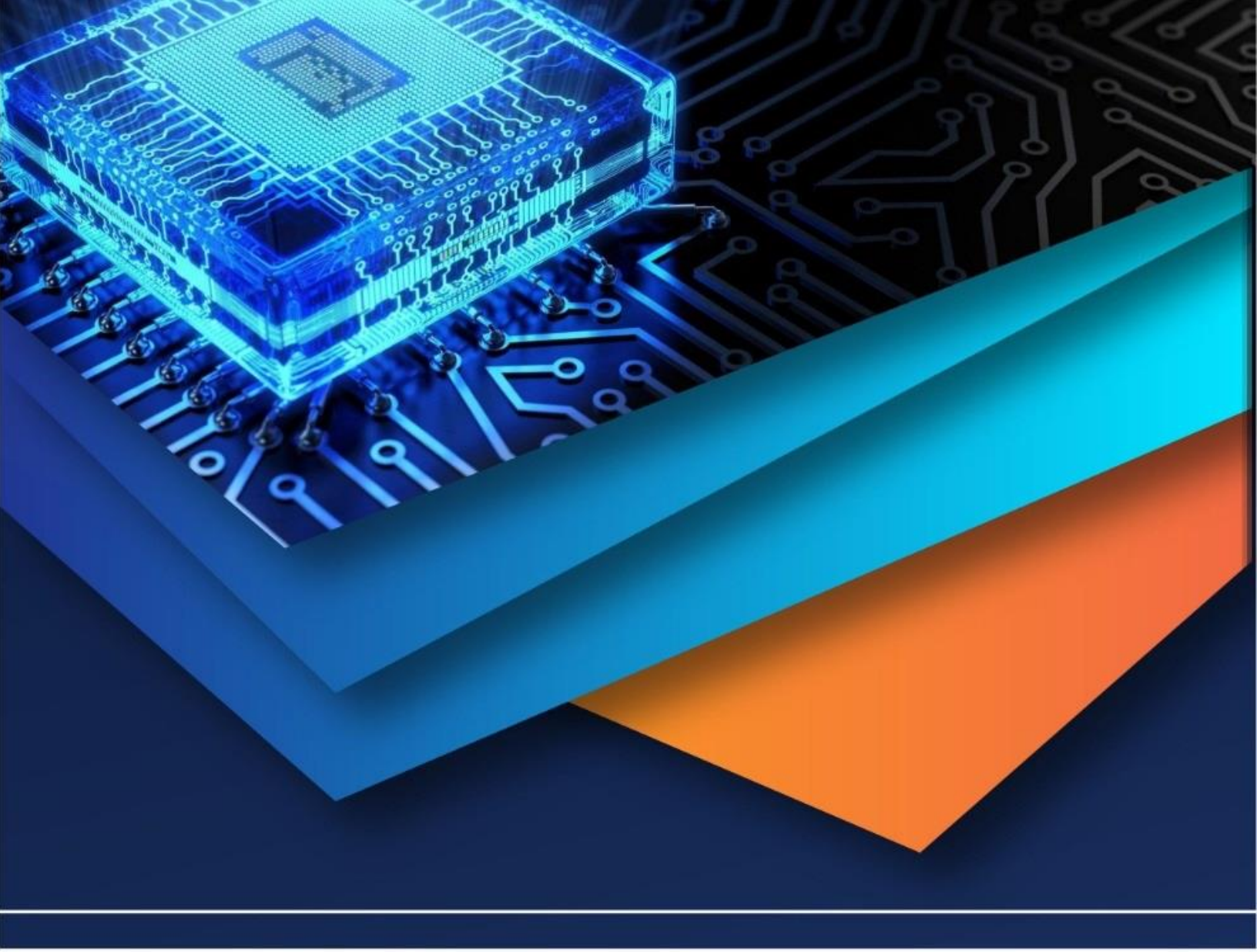
Figure 9: The Decrypted EHR Image 2 And Its Equivalent Histogram Image

V. CONCLUSION

EHR system are necessary to be enhanced with data privacy and private issues. The major cause is to improve the security in electronic health record in the healthcare systems. The performance of EHR is the finest budget solution for any practice. with the technology of EHR, healthcare system can improve quality, safety and capability. The vast client requests EHR permit healthcare system to serve and concern for a patient quicker with any health organization. utility of the system as the electronic health record only accessible to the trusted and respective individuals. The proposed algorithm is developed to verify the security by method of proper encryption and decryption in the Electronic Health Record in the health system. It greatly improves the efficiency of EHR system. The proposed algorithm uses Discrete Cosine Transform(DCT) for image transformation (that is to change the pixel position with less memory).

REFERENCES

[1] Gaspard Harerimana, Jong Wook Kim, Hoon Yoo and Beakcheol Jang, “Deep learning for electronic health record analytics”, IEEE Access,Vol:7,2019.
[2] Gun-Woo Kim and Dong-Ho Lee, “Intelligent health diagnosis technique exploiting automatic ontology generation and web-based personal health record services”, IEEE Access,Vol:7,2019.
[3] Jinghe Zhang, Kamran Kowsari, James H. Harrison, Jennifer M. Lobo and Laura E. Barnes, “Patient2Vec: A Personalized Interpretable Deep Representation Of The Longitudinal Electronic Health Record”, IEEE Access,Vol:6,2018.
[4] Caifeng Zhang, Rui Ma, Shiwei Sun, Yujie Li, Yichuan Wang and Zhijun Yan, “Optimizing The Electronic Health Records Through Big Data Analytics: A Knowledge-Based View”, IEEE,Access,Vol:7,2019.
[5] Zhaori Bi, Mengjing Wang, Li Ni, Guoxin Ye, Dian Zhou, Changhao yan, Xuan Zeng and Jing Chen , “ A Practical Electronic Health Record-Based Dry Weight Supervision Model For Hemodialysis Patients:” , IEEE Journal Of Translational Engineering In Health And Medicine, Vol:7,2019.
[6] Fuhu Deng, Yali Wang, Li Peng, Hu Xiong, Ji Geng, And Zhiguang Qin, “Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records” ,IEEE Access, Vol:6,2018.
[7] Khaled Riad , Rafik Hamza, And Hongyang Yan, “Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records”, IEEE Access, Vol:7,2019.
[8] Rosa Sanchez-Guerrero, Florina Almenarez, Danmiel Diaz-Sanchez, Patrica Arias, Andres Marin “ Collaborative E-Health Meets Security: Privacy- Enhancing Patient Profile Management”, IEEE Journal Of Biomedical And Health Informatics, Vol:21,2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY