Wavelet Based Digital Watermarking Scheme for Medical Images

Mukesh Soni
Jagran Lakecity University,
Bhopal, India
soni.mukesh15@gmail.com

Dileep Kumar Singh
Jagran Lakecity University,
Bhopal, India
dileep.singh@jlu.edu.in

***Abstract*—The transfer of medical images between hospitals is become a normal exercise for better decision making. Digital watermarking has played a very significant role in medical sciences for diagnosis and medication to protect reliability, availability, and confidentiality. Several methods are proposed for medical images using the spatial and transform domain. However, the data falsification ratio is high in the existing mechanisms while exchanging medical images. Hence, we suggest a wavelet based digital watermarking scheme for medical images using three level DWT and BCH coding, which can be used to the medical practitioners for accurate decisions. Security analysis of our proposed work has been done for security assessment, and performance results are discussed to confirm its implementation feasibility in medical sector.**

Keywords: Data; Medical; Security; Watermarking;

I. INTRODUCTION

Digital watermarking is a process of hiding vital information inside the digital data, so that the fixed watermark can be seen or obtained for data confirmation. It has different advantages like theft protection, certain level of marketing, tracking components, and credibility, whereas disadvantages are like interfere in the image, process overhead, and time consuming. To protect digital images, there are four categories as (i) robust watermarking (ii) fragile watermarking (iii) semi fragile watermarking and (iv) hybrid watermarking. Robust watermarking is very hard to eliminate from digital information because they are strong against legitimate or illegitimate activities. They may also be used for copyright protection. Fragile imprints are effortlessly exterminated through tampering, and semi fragile imprints protect information from illicit alterations. Hybrid watermarking is used to achieve accuracy, truthfulness, and ownership safety at once [1].

A. Security Requirements in Medical Images

The most important features required in medical image watermarking are (i) confidentiality (ii) reliability and (iii) availability. Confidentiality indicates that only authorized people can get health data. It can be achieved through encryption, firewall, and access management. Reliability is termed into two parts as integrity (which validates that information is not altered) and authentication (which guarantees that data is provided by a verified source). Integrity is achieved using the encryption mechanism while communicating through images on the network. Authentication needs measurement to find that secrecy and truthfulness of data is not broken. Availability specifies the ability of authorized clients to utilize the information system in typical arranged circumstances [2].

B. Current Watermarking Approaches for Medical Images

Medical images are differentiated in two regions, as region of interest (ROI) and region of non-interest (RONI). ROI comprises the instructive region, considered for diagnostic reason, and it should be saved with no misrepresentation. On another hand, RONI generally signifies the back environment of an image, but it sometimes covers grey level of minor attention. In ROI, spatial or transform procedures is applied to keep information secretly. The encrypted imprint may be strong for human hand images. To retain the integrity of these kind of images, the system avoids the misrepresentation of an image. This ensures that informative part of ROI is not distorted [3].

In spatial domain techniques, the imprint is incorporated in the cover picture by clearly changing the pixel numerical of an original picture. These procedures are straightforward, quick, and present high-level entrenching ability. Furthermore, a minor imprint can be secreted for numerous times. Spatial field methods have some advantages, but then again, their key downside is that they cannot persist counter to various operations like noise increment and lousy compression. Additionally, when uncovering the applied watermarking technique, the secret imprint can be simply distorted by an illegal client. With the current algorithms in the medical field, either there was no ROI and RONI segmentation, or spatial domain was used for digital watermarking [4].

II. LITEATURE SURVEY

Medical images can be easily tampered and can be used for illegal reasons. Thus, researchers came up with various mechanisms to protect medical images from malicious actions while transferring over the network. Wu et al. [5] recommended a block-based approach based on Discrete Cosine Transform (DCT) for watermarking medical images through ROI. But it requires a greater number of computations to recover data for ROI and inserting it into each part of a picture. Mostafa et al. [6] proposed a methodology that saves the Electronics Patient Record (EPR) in an image. This saves

the storing memory, communication cost, and assures protection of information. Watermark embedding is done through the Discrete Wavelet Packet Transform (DWPT). The patent report is employed with an error correcting code, Bose–Chaudhuri–Hocquenghem (BCH) code, to improve the strength of the procedure.

Most of the algorithms proposed have a common problem of security where the watermarks embedded either are not encrypted before embedding or the algorithm used for encryption is weak. Solanki et al. [7] proposed an embedded scheme utilizing RSA technique, and embedded in ROI through Discrete Wavelet Transform (DWT). Fontani et al. [8] proposed that information is embedded using the DICOM regulation, in which the digital signature is positioned in the header. Digital watermarking can be done in such a way that the metadata is robustly linked to the medical image and is not easily distorted. Therefore, they used integer to integer discrete wavelet transform.

Eswaraiah et al. [9] proposed a mechanism to help in removing the image defects, in which an image is separated into ROI, RONI, and border pixels. The median and variation of each ROI part are computed and matched with the average and variance of pixels obtained from subsequent RONI part. Baiying et. al. [10] proposed a reversible watermarking technique with wavelet transforms and singular value decomposition (SVD). Signature and logo are implanted by recursive dither modulation procedure (RDM). Differential evolution (DE) is applied to suggest the quantization steps optimally for better robustness and capacity. Shabir et. al. [11] has proposed the practice of pixel to block conversion technique (PTB) to increase capability, as it is computationally effective method for making covering picture from an input image. Block checksum calculation helps in manipulate finding and localization. The main disadvantage is that the imprint implanted in an image is unstable.

Parah et. al. [12] has introduced a watermarking approach for health-related images by proposing two algorithms, as first one is the electronic patient record (EPR), and the imprint is inserted in an entire image. The process of the second algorithm is as, the imprint is implanted in the RONI part of an image. The suggested procedures are executed in DCT through 8×8 block wise. The disadvantage of inserting in a whole image is that the watermark can misrepresentation an image to that point, where it is hard to distinguish it due to alterations. Medical practitioners refuse to diagnose images that have been distorted even a little bit. When imprint is embedded in only RONI part of an image using DCT, the main disadvantage is as there is no protection against picture adjustment. One of the main difficulties and the criticism of the DCT is the blocking process. In DCT, imageries are divided in 8x8 or 16 x 16 blocks or bigger. The concern with these blocks is that when an image is altered to greater compression ratio, they are detectable, and it is named as the blocking process.

Ali et al. [13] came with an approach to achieve secrecy, genuineness, and truthfulness for the pixel and header data, using the crypt-based mechanism. As the procedure involves encryption and signature construction method and decryption and signature confirmation technique, and they require more time rather than projected. Soualmi et al. [14] designed a mixture of DCT transform, weber descriptors (WDs), and Arnold chaotic map. In this, the imprint image is firstly twisted using Arnold chaotic map. After that, DCT is executed on each image block, and watermarked information is fixed in the DCT middle-band coefficients of all blocks. Lastly, a new implanting and obtaining method is projected, using WDs without losing by choosing the appropriate coefficients. Al-Haj et. al [15] came up with an approach based on DWT, and this method achieves better results in higher PSNR value. Thus, it offers high ranking validation contrasted to the exiting approaches.

Al-Nabhani et al. [16] proposed an undetectable blind watermarking mechanism using probabilistic neural network. The suggested procedure aims to sustain the hiddenness and superiority of a watermarked picture by choosing the finest inserting spots in the block-based wavelet measurement. Liu et al. [17] came up with a multi-watermarking system, in which the graphical feature trajectory of an image is firstly extracted using dual-tree complex wavelet transform and discrete cosine transform (DTCWT-DCT). After that, the watermark data is improved through henon map chaotic encryption.

III. BACKGROOUND

A. System Model

A sender sends the watermarked image that has the watermark encoded by a secret key. Watermark consists of patient's information, doctor's information, diagnostic information of that patient, least significant bits (LSB) of ROI part of a Health-related data image and logo that is additionally stored to check integrity. The receiver receives the watermarked medical image and removes the watermark by using an extraction algorithm and uses the same key to decode the watermark that had been embedded in the watermarked image. Figure 1 gives an overview of the process of medical images transmission and extraction.

B. Problem Statement

Watermarking techniques that applied in spatial domain for embedding data, which have the disadvantage that is as, it works with a picture plane itself, while the frequency field deals with the rate of pixel shift. It also lacks robustness and can be easily attacked by geometric attacks. When DCT is considered for health information images through watermarking, it is more time-consuming as it involves a number of computations to extract vital data and insert it into blocks of medical pictures. When a medical image has not been splitted into ROI and RONI and instead medical data has been embedded into the whole image leads to high distortion of the ROI part of a health-data image. Due to high distortion, medical practitioners would refuse to diagnose based on that medical image [1], [2].

Therefore, we require a watermark technique that provides us a stronger imprint that can be inserted with no compromising the merit of a medical image, and it should be done in less time, as well as taking less computing power.

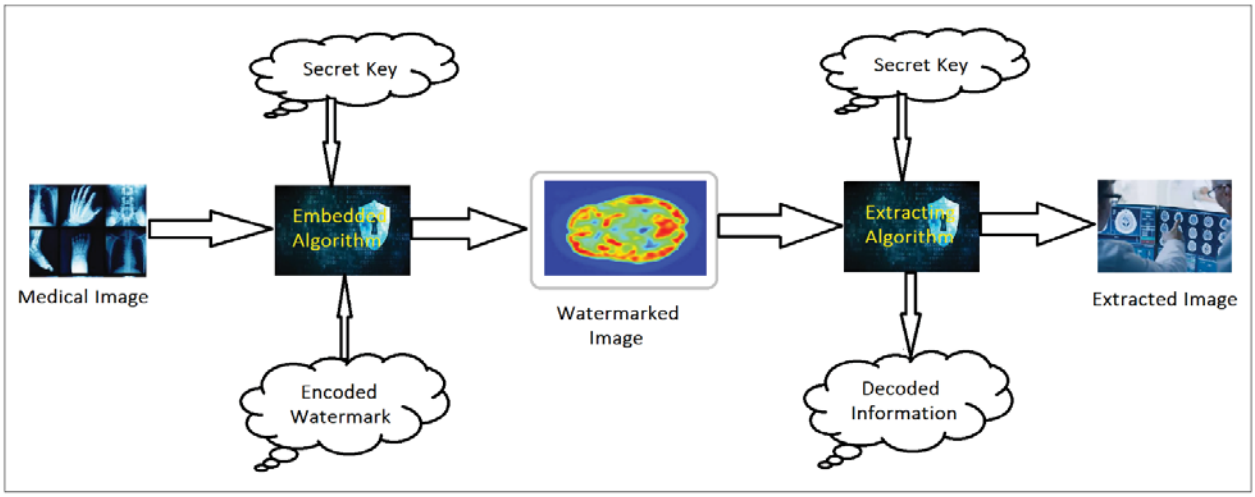

Figure 1. The system model overview

IV. The Proposed Solution

We propose a wavelet based digital watermarking system by achieving security requirements. Specifically, we have used three level DWT along with the BCH coding, which improves the mechanism further undetectable and powerful to counter different threats. Three level DWT is performed on the RONI of a health-information image so it can produce distinct frequency sub-bands (LL, LH, HL, HH) after every stage of separation. The encoding of a picture is done in the non-overlaying blocks of a LL sub-band. After embedding the watermark, we perform three level inverse DWT transform to get a watermarked picture for health data to achieve confidentiality, availability, and reliability for transferred images. Firstly, we explain the recommended embedding procedure and then, extraction process.

All the information that needs to be sent across to the receiver as part of watermark has been done by BCH encoder, as it generates a BCH cipher (it is used as cyclic error correcting codes, constructed by polynomials in a finite field. One of the vital aspects of BCH codes is that there is an accurate regulator on the count of representation inaccuracies adjustable through the code in the code construction. It is conceivable to create binary BCH codes that can fix numerous bit faults. Further, BCH code is a comfort, which can be deciphered, by using an algebraic technique (called as syndrome decoding). In this approach, it elucidates the model of the decipherer for these procedures, based on a little low-power automated hardware. Ultimately, the proposed system is constructed based on the combination of three level DWT and BCH coding to satisfy the vital security requirements. Figure 2 indicates the suggested imprint embedding algorithm, and the process of original image recovery is shown in Figure 3.

A. Watermark Embedding Scheme

- In ROI part of the image, a fragile watermark is introduced using LSB algorithm. The LSB algorithm introduces the imprint for a health image by altering LSBs of a grey scale picture.
- The original LSBs of the ROI part along with patient information, doctor's information, diagnostic information, and logo are first encoded using secret key and then inserted into the RONI region of a medical picture as a powerful imprint.
- RONI region is primarily divided into N X N blocks and then subjected to a 3-level DWT. After this, the robust watermark generated from above is inserted into the image. The image is then subjected to 3-level Inverse Discrete Wavelet Transform (IDWT) to bring it back to spatial domain. Finally, the ROI and RONI zones are merged to obtain an imprinted picture, which is already sent to the receiver.

B. Watermark Extraction Scheme

- The watermarked image received from the sender is splitted in ROI and RONI parts.
- The RONI part is divided into N x N blocks and subjected to 3-level DWT. Further, it is extracted and decrypted to get back patient information, doctor's information, diagnostic information, and logo along with the LSBs of the ROI region. The doctor's information helps to check the authenticity and logo to test the truthfulness of a picture.
- In ROI portion, the fragile imprint is extracted to test the precision of a picture, and LSBs are obtained from a potent imprint, which is employed to switch bits in ROI portion to recover an initial non-altered picture.
- The RONI portion is subjected to 3-level Inverse DWT and then combined with the ROI part to retrieve an initial health-information image.

V. Security Analysis

Security analysis of our proposed work has been done to check its security strengths against different security parameters. Further, we discuss the powerfulness of the suggested approach to counter various incidents.

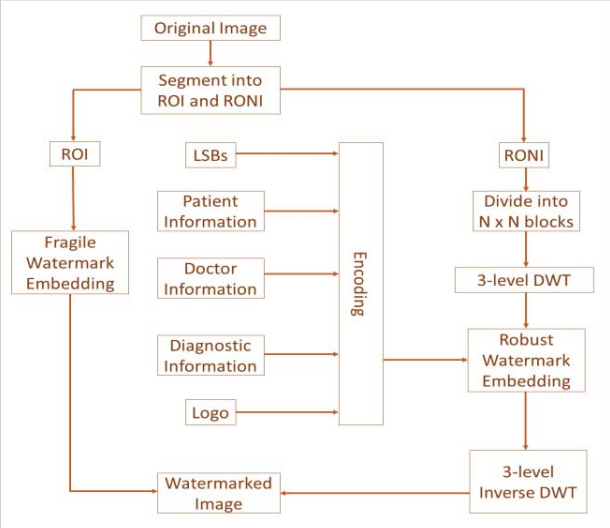

Figure 2. The process of watermark image embedding

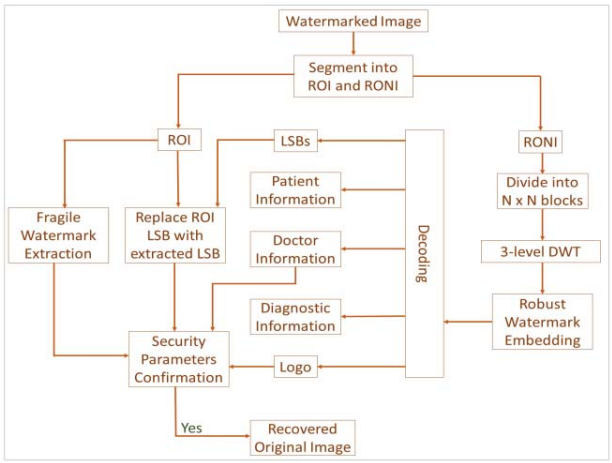

Figure 3. The process of original image extraction

A. Security Parameters

Confidentiality has been achieved by generating two keys. The first key is a 256 X 256 matrix that has been used to embed information at the first level of DWT decomposition. This key has been generated by combining RONI part of image (converted into matrix form) and a random matrix of size 256 X 256 that has been separately generated. The second key is a 128 X 128 matrix that has been created from the key that has been computed above.

Reliability is divided into Integrity and Authentication. Integrity is achieved by embedding a logo along with all the information that needs to send with a health picture as part of watermark. Whenever the imprinted picture is manipulated, the extracted logo will show some forgery. Thus, the receiver know that the image has been tampered with and will then provide integrity to the image. Authentication is provided by keeping both (client and doctor) vital data in an image.

B. Security Attacks

To check the security of the proposed solution, we apply few security attacks in the system.

1) *Gaussian Noise:* It is a procedure in which noise signals are inserted to a health-information containing image so that it is purposefully fallacious an image. Therefore, it decreases its graphical feature.

2) *Salt and Pepper Attack:* It has an incredibly unique probability distribution function to Gaussian noise. It denotes the subject as arbitrarily happening for white and black pixels in a health-information enclosing picture.

3) *Median Filtering Attack:* It is an illustration managing procedure, which intends to diminish the existence of noise in a vital information comprising image. As a result, it enriches the picture merit. The hypothetical rationale in the system by using median filter is consideirng various picture properties. So the imprinted signal acquires when it is available in its host. Any watermark waves can be measured as a little differing indication within its part. The power of this indicator is similar to highly noisy in any picture taking component. As a median filter eliminates noise existence, it is anticipated that a few imprint signal appear in a health-information comprising picture will as well be influenced or eliminated.

4) *Gaussian Smoothing Attack:* Gaussian smoothing is used to share several shared vital properties with other leveling procedures like median filtering. It is a picture managing method, to decrease the occurrence of noise in a health-informtion contaning picture to increase its excellence. The motive behind the usage of the gaussian smoothing procedure to infect imprints is related to that of the median filter. The variation among gaussian smoothing and median filtering remains on the approach the leveling is conducted. Gaussian smoothing filter is a minimal route frequency filter, where median filter is a changing a pixel numbers by the subjective median of the power level in the region specified by the filter mask.

5) *Modification:* Modify some of the bits of the watermarked image so that the data stored in it has changed. Thus, if anyone attempts to change any information in an image, then it is idenitfied immediately.

VI. Performance Analysis

It is needed to protect the quality of health-information containing images. To check the performance of the suggested approach, we should confirm the exactness of a recovered picture. The results are presented against the following benchmarks:

A. Peak Signal to Noise Ratio (PSNR)

PSNR is an illustration to find the relationship among the highest achievable value of a signal and the influence of altering noise. It impacts the image accuracy, as it is related to its representation. If PSNR is high, then it indicates that there is more similarity between both pictures.

B. *Signal to Noise Ratio (SNR)*

SNR is described as the proportion of signal power and noise power, which is measured in decibels. A higher ratio (greater than 0 dB) implies incremented signal than noise.

C. *Mean Squared Error (MSE)*

It is the average squared change between the projected and the genuine numbers, as median of the square's errors.

The above performance measures are useful to decide the efficiency of the scheme for implementation in the network. Therefore, we have implemented the suggested system in MAT Lab software to get the results analysis, so it is clear to the receiver party regarding any alterations in transferred images. If any changes in the pictures, then it reflects in the above-mentioned measures directly. Hence, it is easier to determine whether any modifications are done or not. To assure the results, we calculate PSNR, MSE, and SNR using C programming language codes for different relevant mechanisms and the proposed system. Further, we do the comparison of PSNR and SNR for the existing relevant mechanisms and the proposed scheme, in Figure 4. If the outcome of PSNR and SNR is high, then there are less chances for any variations in the pictures. The MSE is 0.0075 in [15], 0.0109 in [16], and 0.0012 in the suggested mechanism. It is better to have low MSE in the results, as it dictates the possible error rate in the pictures.

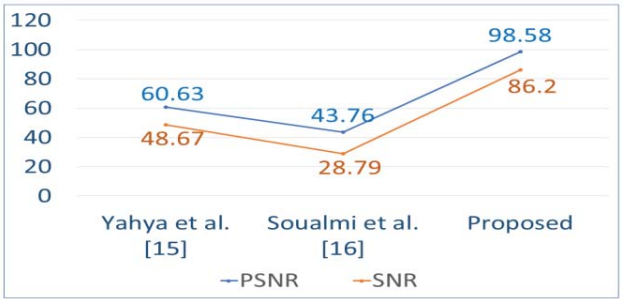

Figure 4. PSNR and SNR Comparison for Schemes

VII. CONCLUSION

The requirement of keeping safe health-information containing images and other relevant client's records are not only for secrecy objective, but as well as to avoid falsifications, which generally occur by permitted and illegal entities while dealing with this kind of images. Many methods are suggested to defeat different difficulties. Experiments favor DWT based methods, as it achieves a precise corresponding to the human visual system. Medical needs are exceptionally rigorous with the superiority of health-information pictures, and it does not permit non-scientific based change. Our proposed solution tries to meet all security requirements, as mentioned in the problem statement. Further, the execution results appear that the performance of the suggested mechanism is better while taking security needs into account. Hence, the potential capacity of this work is to make it more attack resistant while sending crucial images in a public environment.

REFERENCES

[1] Qasim, A. F., Meziane, F., & Aspin, R. (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. Computer Science Review, 27, 45-60.

[2] Mohanarathinam, A., Kamalraj, S., Venkatesan, G. P., Ravi, R. V., & Manikandababu, C. S. (2019). Digital watermarking techniques for image security: a review. Journal of Ambient Intelligence and Humanized Computing, 1-9.

[3] Qasim, A. F., Aspin, R., Meziane, F., & Hogg, P. (2019). ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images. Multimedia Tools and Applications, 78(12), 16433-16463.

[4] Abraham, J., & Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. Journal of King Saud University-Computer and Information Sciences, 31(1), 125-133.

[5] Wu, J. H., Chang, R. F., Chen, C. J., Wang, C. L., Kuo, T. H., Moon, W. K., & Chen, D. R. (2008). Tamper detection and recovery for medical images using near-lossless information hiding technique. Journal of Digital Imaging, 21(1), 59-76.

[6] Mostafa, S. A., El-Sheimy, N., Tolba, A. S., Abdelkader, F. M., & Elhindy, H. M. (2010). Wavelet packets-based blind watermarking for medical image management. The open biomedical engineering journal, 4, 93.

[7] Solanki, N., & Malik, S. K. (2014). ROI based medical image watermarking with zero distortion and enhanced security. International Journal of Education and Computer Science, 10, 40-48.

[8] Fontani, M., De Rosa, A., Caldelli, R., Filippini, F., Piva, A., Consalvo, M., & Cappellini, V. (2010, September). Reversible watermarking for image integrity verification in hierarchical pacs. In Proceedings of the 12th ACM workshop on Multimedia and security (pp. 161-168).

[9] Eswaraiah, R., & Sreenivasa Reddy, E. (2014). Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI. International journal of telemedicine and applications, 2014.

[10] Lei, B., Tan, E. L., Chen, S., Ni, D., Wang, T., & Lei, H. (2014). Reversible watermarking scheme for medical image based on differential evolution. Expert Systems with Applications, 41(7), 3178-3188.

[11] Parah, S. A., Ahad, F., Sheikh, J. A., & Bhat, G. M. (2017). Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. Journal of biomedical informatics, 66, 214-230.

[12] S.S. Bedi, G.S. Tomar & Shekhar Verma, "Robust Watermarking of Image in the Transform Domain using Edge Detection", IEEE International Conference on simulation UKSIM 2009, pp.233-238, Mar 25-29, 2009.

[13] Parah, S. A., Sheikh, J. A., Ahad, F., Loan, N. A., & Bhat, G. M. (2017). Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimedia Tools and Applications, 76(8), 10599-10633.

[14] Ali, M., Ahn, C. W., & Pant, M. (2014). A robust image watermarking technique using SVD and differential evolution in DCT domain. Optik, 125(1), 428-434.

[15] 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.

[16] Yahya, A. N., Jalab, H. A., Wahid, A., & Noor, R. M. (2015). Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. Journal of King saud university-Computer and Information sciences, 27(4), 393-401.

[17] Soualmi, A., Alti, A., & Laouamer, L. (2018). A new blind medical image watermarking based on weber descriptors and Arnold chaotic map. Arabian Journal for Science and Engineering, 43(12), 7893-7905.

[18] Liu, J., Li, J., Ma, J., Sadiq, N., Bhatti, U. A., & Ai, Y. (2019). A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and Henon map. Applied Sciences, 9(4), 700.