Engineering and Technology Journal
Journal homepage: engtechjournal.org

Secured Medical Image Hashing Based on Frequency Domain with Chaotic Map

Amira K. Jabbar [a]*, **Ashwaq T. Hashim** [b] , **Qusay F. Al-Doori** [c]

[a] Control and Systems Engineering Department, University of Technology, Baghdad, Iraq, 60781@student.uotechnology.edu.iq

[b] Control and Systems Engineering Department, University of Technology, Baghdad, Iraq, 60102@uotechnology.edu.iq

c Control and Systems Engineering Department, University of Technology, Baghdad, Iraq, Qusay.f.hasan@uotechnology.edu.iq

* Corresponding author.

Submitted: 05/08/2020 Accepted: 19/12/2020 Published: 25/05/2021

KEYWORDS

CSK ,Chaotic map, DCT, Integrity, Medical image SLT.

ABSTRACT

Recently, online-medicine got increased global interest, particularly during COVID19 pandemic. Data protection is important in the medical field since when promoting telemedicine applications, it is necessary to protect the patient data and personal information. A secured process is needed to transmit medical images over the Internet. In this paper hash algorithm is employed to protect the data by using powerful features from the coupled frequency domains of the Slantlet Transformation (SLT) and the Discrete Cosine Transform (DCT). The Region of Interest (ROI) is localized from an MRI image then extraction of a feature set is performed for calculating the hash code. Then, hash code is enciphered to maintain security by employing a secure Chaotic Shift Keying (CSK). The suggested method of security is ensured by the strength of the CSK and the encryption key secrecy. A detailed analysis was conducted using 1000 uncompressed images that were chosen randomly from a publicly available AANLIB database. The proposed methodology can be useful for JPEG compression. Also, this method could resist many attacks of image processing likes filtering, noise addition, and some geometric transforms.

How to cite this article: A. K. Jabbar , A. T. Hashimb, and Q. F. Al-Doori "Secured Medical Image Hashing Based on Frequency Domain with Chaotic Map," Engineering and Technology Journal, Engineering and Technology Journal, Vol. 39, Part A, No. 05, pp. 711-722, 2021.
DOI: https://doi.org/10.30684/etj.v39i5A.1786

1. INTRODUCTION

In the healthcare system, medical imaging takes an essential role as it helps in diagnosis and decision-making. Enormous advance in technologies of information and communication has made it easier to access, modify, and distribute digital data. Because of the threats of security through communication between any data point, the medical images must be exchanged in a preventive manner, and therefore the medical data management is achieved through many medical information issues such as authentication, security, safety, privacy, and others. Sensitive patient data also requires the privacy and integrity of data for ensuring the reliability of the data. While in contact, medical images can be vengefully manipulated by inserting or removing a lesion that leads to the wrong diagnosis by the doctor. The primary attention of authors in this community is for offering novel ways to address the mentioned issues smoothly and efficiently [1].

There are many techniques available in the literature that can guarantee the security and privacy of medical images. These techniques include encryption [2][3][4], watermarking[5][6][7], image signature or hash [8], and encryption provides images protection; when decrypted, the safety is lost, while the watermarking can detect if the integrity of images is at risk. Integrity-based cryptographic hash methods are verified the precise identity or content of images. Li and Preneel [9] proposed a hash algorithm for the image which is offered block-level content protection. It employs the Discrete Fourier Transform (DFT) to extract features from coefficients of image blocks. This method provides a verification level to safeguard the whole content compared with the traditional hash algorithms of images which only offered a limited verification level to protect the whole content. Huang et al., [10], used a Tchebichef moment combined with DCT to medical image authentication. A set of suggested features is named after the histogram statistics for block-based Tchebichef moments are reorganized. The proposed method does not merely discover whether the test images have endured an alteration comprehensive; nevertheless, it also discovers the nature of the amendment. Desai and Rao [11] suggested an approach to generate image hash code based on neural networks. Three sample images have been taken and their hash values are calculated using two structures of neural network. The first one is a structure without feedback and the second is a structure with feedback. Then the original images are subjected to bit adjustment, Gaussian noise, and rotational noise. The hash codes to the modified images are recalculated. Quattrox et al. [12] provided a system for checking the integrity of the medical image to detect and approximate harmful local adjustments to the image, as well as determine the nature of the global processing to which the image might be exposed. This system tries to find out the motives for tampering, but it is still limited to revealing predefined types of images or tampering. Ranjani and Babu [1] proposed a method to verify the medical image content where the hash signatures from the medical image are computed by singular value decomposition (SVD). Then the hash signature is embedded in the region of non-interest (RONI) of the image by the suggested sequential square encoding (SSE) method. In the research of Eswaraiah and Reddy [13], the medical image was divided into ROI and RONI regions. The Hash code is produced from the ROI and then embedded in the RONI area beside the ROI recovery data and patient's information by integer wavelet transform. This technique needs the provision of the physician to mark the ROI and to separate the RONI. However, it is almost difficult to mark the same area while extracting the watermark. Akkasaligar and Biradar [14], proposed an integrity approach using SHA-256, Deoxyribonucleic Acid (DNA) encryption, and a chaotic map. For integrity initially, the code of hash is produced by SHA-256 and is concealed in the Least Significant Bit (LSB) of digital medical image. DNA coding rules are used to encrypt the image for safety. The coded DNA pixels matrix is scrambled and diffused by a hyperchaotic map, Chen. After the above discussion, developing a robust image hash scheme for all kinds of content saves, sensitive for little level manipulation, and safe is a very difficult job. Some papers reviewed above work very well to harmless lesions, on the other hand, cannot sense little level manipulation. Most papers do not secure hashes, making it difficult to use hashes to authenticate images. If the hash is produced without retaining a secret key, the attacker can launch hash collision attacks to defeat the primary image authentication purpose [15]. Based on the literature survey, it is concluded that to date, no standard has been established for image hashing schemes because there is always a trade-off between strength and discriminatory ability.

This paper is aimed to suggest a powerful hashing function that esteems the design philosophies and overall image hashing algorithms features. A feature set is employed for computing a perceptual hash value. A chaotic system is used to encrypt the hash value. The achievement of the suggested system is specified by the construction of the feature set and the employment of a secure chaotic system to encode the feature set. The proposed algorithm is likely to be able to resolve copyright disputes, authenticate analogous images, and retrieve image content from big image databases.

2. THE PROPOSED SYSTEM

The proposed method presents a scheme of image hashing for the medical image using a group of powerful extracted features from coupled frequency domains of DCT-SLT and then encrypting the generated group of features by a CSK system. At first, the ROI is extracted from the MRI image then the hash value is computed, at last, the system will encrypt the hash value by employing the CSK as depicted in Figure 1.

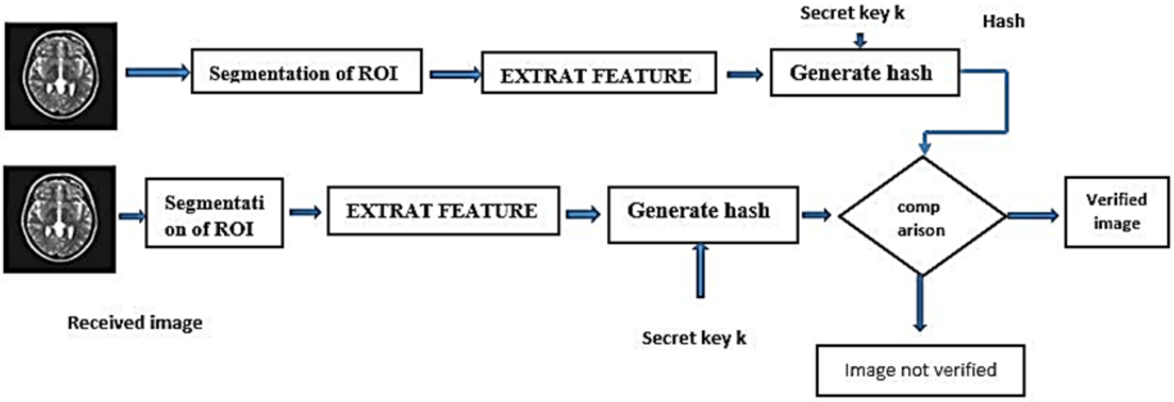


Figure 1: The block diagram of the proposed system

I. Segmentation of Region of Interest (ROI)

During the first step, the RONI region of the medical image is to be eliminated like a brain image that is presented outside of the skull. For doing so, the boundary of the skull is identified by the aid of enhancement techniques with automatic global thresholding technique, morphological operations are used to remove the unusable parts of the skull that existing outside to it. Algorithm 1 illustrates the steps of ROI localization:

```
Algorithm 1: ROI Localization
Input:
    MI,    // Medical image
   W, H    // Width, and Hight
Output:
   ROImg    // localized ROI region
Step1: Read medical image MI of size W×H
Step2: Enhanced intensity values of MI by applying contrast stretching using the following formula:
```

$$E(x,y)= \begin{cases} 0 & IM\,(x,y) \le \text{Low} \\ 1 & \\ 255\times \frac{I(x,y)-Low}{High-Low} & \text{Low}<IM(x,y)< \text{High} \\ 255 & IM(x,y)\ge \text{High} \end{cases} \tag{1}$$

Where *E(x,y)* is the image after enhancement, *IM(x,y)* is the input medical image. The values of Low and High have been selected by trial and error. The value of Low is 0.0902 and the value of High is 0.9490.

Step3: Gamma mapping operator is applied to the image *IM* using the following equation:

$$G = ((IM/255)^\wedge\alpha) \times 255 \quad (2)$$

Where *G*: a gamma image, *IM*: the medical image, and α: the gamma factor. When the values of α lie in the range of 0-1, it enhances the contrast of the bright regions, and when α is bigger than 1, it enhances contrast in the dark regions. The value of α= 2.5 is selected to make the medical image brighter and to let the ROI region more distinguished. This value is suitable for the best results in this step.

Step 4: Compute the threshold *TH* value by the following formula:

$$TH = \text{Initial\_Value} + (\text{Max(IM)} + \text{Min(IM)}) / 2 \quad (3)$$

Where Initial_Value=10.

Step5: Apply threshold on the medical image such as the following:

$$Binary(\mathrm{x,y}) = \begin{cases} 1 & MI(x,y) \geq TH \\ 0 & MI(x,y) < TH \end{cases} \quad (4)$$

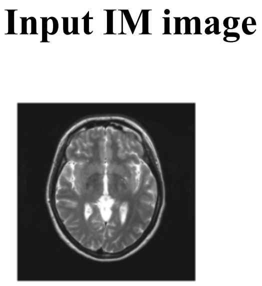
Use the Morphological closing operator for a binary image *Binary*. The closing filter operation will smooth the boundaries, decreases small inner collisions, tie narrow joints, and fill small holes resulted from the noise.

Step7: Traces the exterior boundaries of *Binary* by the *bwboundaries* function in Matlab which is implemented using the Moore-Neighbor tracing *algorithm*.

Step8: Compute the four sides (i.e., up, down, left, and right) and determine the first white pixel on each side. When scanning horizontally and vertically, let $x_{L,}$ $x_{R,}$ x_T, and x_B are the first white pixels to the left, right, down, and up directions respectively.

Step9: Isolate the ROI from the original image (i.e, IM).

The flowchart of the proposed ROI localization is shown in Figure 2 while the output of each step for proposing ROI localization is depicted in Figure 3.



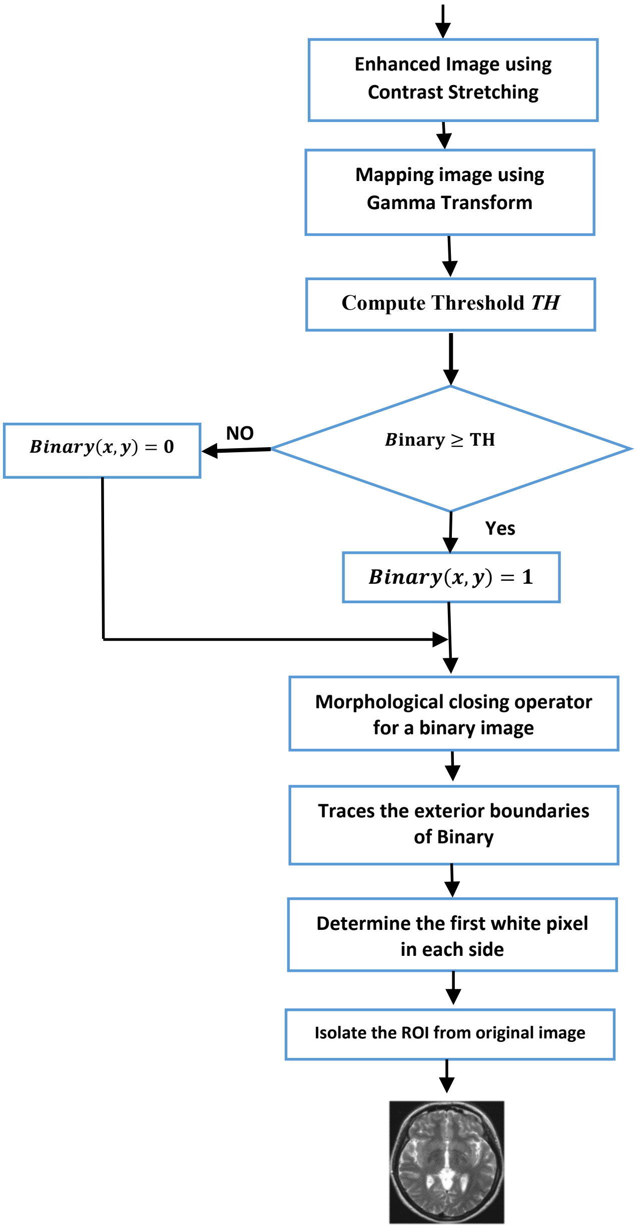

Enhanced Image using Contrast Stretching
Mapping image using Gamma Transform
Compute Threshold TH
$Binary \geq$ TH
NO
$Binary(x, y) = 0$
Yes
$Binary(x, y) = 1$
Morphological closing operator for a binary image
Traces the exterior boundaries of Binary
Determine the first white pixel in each side
Isolate the ROI from original image

Figure 2: Flowchart of ROI Segmentation

Figure 3 shows the steps of ROI localization and Figure 4 shows some samples of the brain data set.

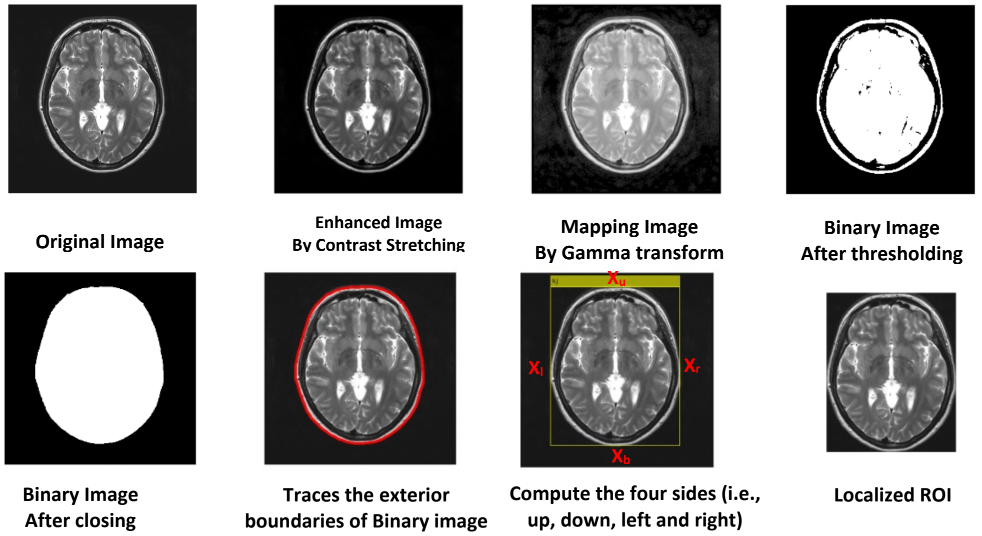


Figure 3: Steps of ROI localization for the brain image

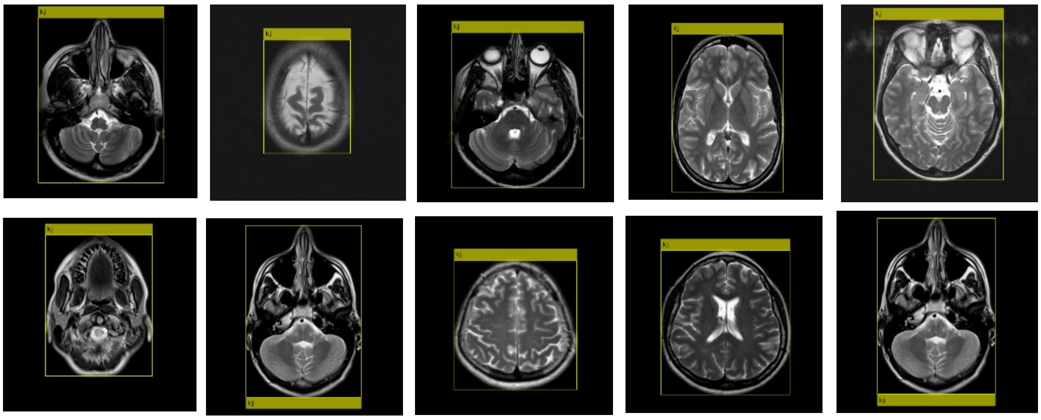


Figure 4: Samples of ROI localization for the brain dataset

II. Extracting Features

In the proposed system the ROI, sub-image is resized to get a squared sub-image and is divided into m × m pixels block size. Hash code is generated by calculating the signatures of each block. SLT and DCT are employed together to extract the essential features set. The SLT first level decomposition confirms the isolation of the gray image information in frequency sub-bands LL_1, HL_1, LH_1, and HH_1. The LL_1 sub-band holds most of the information from the gray image. Therefore, we take into consideration the LL_1 sub-band for the feature extraction method. Decomposition is achieved at the n-level, taking into account the LL_{n-1} sub-band ($n \geq 2$) in each iteration. When decomposing to the n-level, the LL_n sub-band is obtained and the LL_n offers a square array that preserves most of the correlation from the original gray image. This sub-band is divided into blocks of size k×k and then the DCT transform is applied for these blocks. According to the DCT distribution, the block top-left corner holds the high frequencies while the bottom-right holds the low significant frequencies. Each block has a DC term, i.e. the (0,0) frequency, which includes the most block significant information part. This term is taken from each DCT block and is used to form the hash code.

A feature vector of DC's is obtained for all computed DCT blocks from the LL_n subband. Subsequently, the feature vector is binarized and this is accomplished by comparing each feature set component with the overall set of feature average. Binary 0 is employed to state DC values below the average and binary 1 is employed to state the DC values exceeding average. Consequently, a binary hash code is obtained for the digital image as shown in Figure 3. The image segmentation system proposed is described in Algorithm 2.

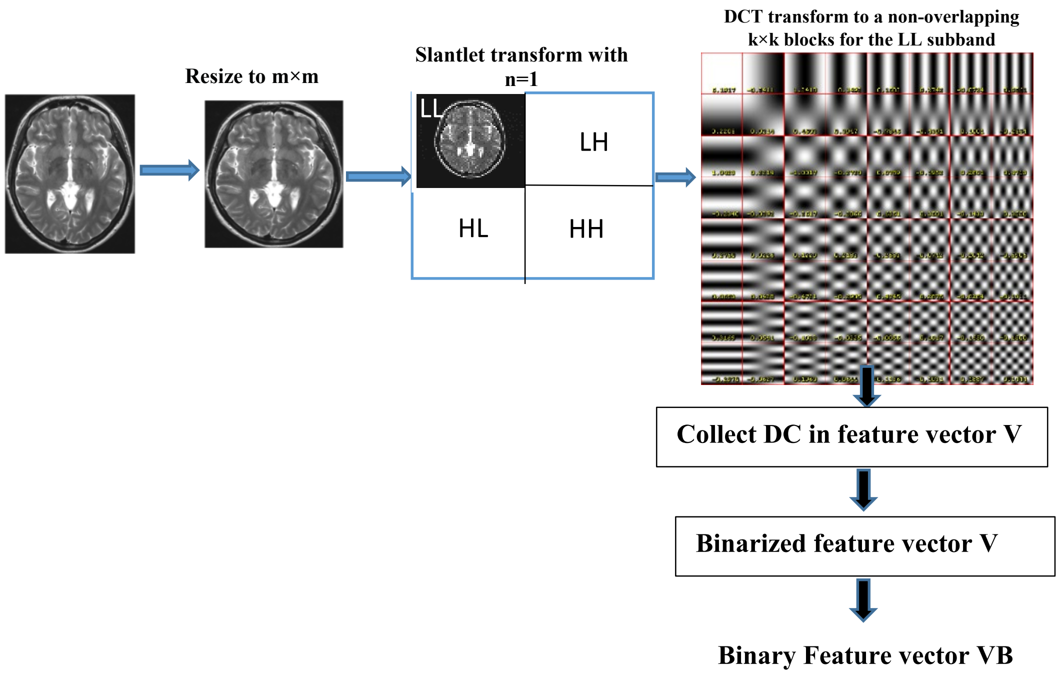

Resize to m×m
Slantlet transform with n=1
LL
LH
HL
HH
DCT transform to a non-overlapping k×k blocks for the LL subband
Collect DC in feature vector V
Binarized feature vector V
Binary Feature vector VB

Figure 5: Block diagram of the proposed extract feature

Algorithm 2: Extract Feature

```
Input:
    ROIimg,   // Region of interest image
    W, H      // Width and Height
    n,        //number of level
    k,        // block size
    m         // The new size of image
Output:
    VB        //  Binary Feature Vector
```

Step1: The gray image ROIimg is resized to m×m dimensions by the bicubic interpolation.

$$ROIimg(\mathrm{x,y}) = \mathrm{BicubicResize}(\mathrm{ROIimg}(\mathrm{H,W,[m,m]}))\ if\ H\ or\ W < 256 \tag{5}$$

Step2: Apply 2D SlantLet Transformation (SLT) with n level

Step4: The n LL sub-band is split into the non-overlapping k×k blocks and then apply the DCT transform on each block.

Step5: The DC terms are collected from all blocks of DCT to construct features vector V of the ROIimg. The length L of the features vector V is calculated using the following formula:

$$\mathrm{L= ((m/\ (k.2))\ \hat{}n)\ \hat{}2} \tag{6}$$

Step6: Compute the mean value m_{dc} for the features vector V.

Step7: Binarized the features vector V to get binary features vector BV using the following formula:

$$BV_I = \begin{cases} 0 & Vi < m_{dc} \\ 1 & Vi \geq m_{dc} \end{cases} \tag{7}$$

V=(V_i) and BV=(BV_i) where i=1,.., l

III. Feature Enciphering

This step is required to maintain the binary feature set security. The security is accomplished by encryption by a Chaotic Shift Keying (CSK) system. In binary CSK modulation, signals of chaos are used to transmit the binary information carrying different bit energies A digital symbol is encoded by sending one signal of chaos $x_1(t)$ or $x_0(t)$ at a time. For example, for a binary bit of signal "1" during the time t is to be sent, x1(t) is transmitted, and for a binary bit "0", $x_0(t)$ is to be transmitted. Both of the chaotic signals $x_1(t)$ and $x_0(t)$ can emit from the same system with different parameters or two different chaos systems. In our work, we focus on the modulation technique of antipodal CSK [16]. Where the two random sequence signals used are the inverted version of each other ($x_0(t) = -x_1(t)$). The CSK signal using Quadrate map [17] that the transmitted signal can then be written as:

$$s(t) = \begin{cases} x_1 & symbol\ 1\ is\ transmited \\ x_0 & symbol\ 0\ is\ transmited \end{cases} \tag{9}$$

Figure 6 depicts the feature vector enciphering block diagram and Figure 7 shows the Quadrate mapping.

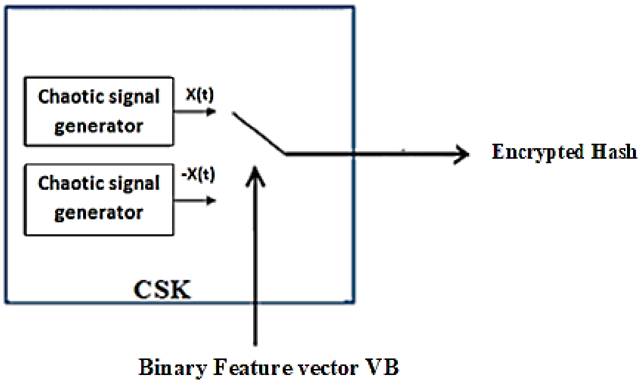


Figure 6: Block diagram of the features vector enciphering

At the receiver, the same random chaotic sequence S is generated using the same initial condition that used in the sender, and then the Hash is reconstructed. Figure (7) depicts the features vector deciphering block diagram

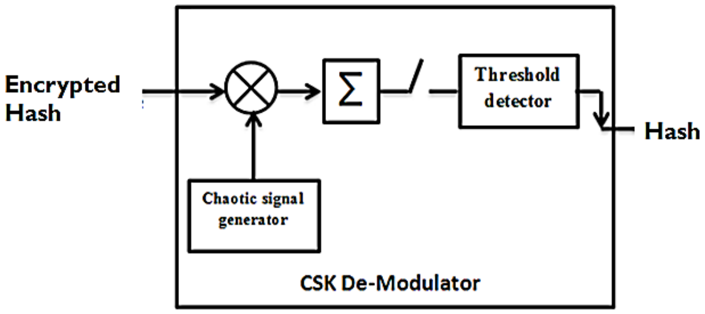


Figure 7: Block diagram of the feature vector deciphering

3. EXPERIMENTAL RESULT

The proposed algorithm is investigated using 1000 uncompressed images with BMP format that are randomly selected from a publicly available AANLIB database of Harvard medical school [18]. All the *images* in the *database* are MRI having a *dimension* of 256 × 256 pixels. Numerous parameters are confirmed during the simulations like the resized image dimension (m), n–level for the SLT transformation, and the size of block k×k for the DCT transformation. The performance of the algorithm is tested under the subsequent parameters: m=256, n=1, k=8, and L=256. The length of binary hash code L=256 is investigated when performed the proposed algorithm with the mentioned parameters. The bit error rate (BER) is used as a metric to measure the distance between hash values and it is defined as:

$$d_{xy} = \frac{1}{N}\sum_{i=0}^{N-1}|x_i - y_i| \tag{8}$$

where x and y are two binary vectors of length N.

I. Robustness Test

A good algorithm is robust against legitimate distortion. We consider a few kinds of distortion as legitimate – JPEG compression, scaling, median smoothing, Wiener Filtering, rotation, and Sharpening. They are commonly encountered in practice. The hash value is expected to be insensitive to these operations. For each pair of the original image and its distorted version, we compute the average hash distance. The results are listed in Table I.

TABLE I: Robustness against attacks

Attacks	**Propose d method**	**Ref 19**	**Ref 20**	**Ref 21**	**Ref 22**
Wiener Filtering	0.0039	-	-	-	0.0039
Median Filtering	0.0125	-	-	-	0.0156
Sharpening	0.0121	-	-	-	0.0117
Sample Down	0.0542	0.124	0.096	0.065	-
JPEG compression	0.0365	0.189	0.037	0.168	0
Rotation 10^0	0.0367	0.125	0.067	-	0.4961
Scale 40%	0.0086	0.149	0.135	-	0.0117

The suggested hashing method was implemented well under filtering, Sharpening, and some geometric attacks compared with some related researches[9][19][20][21]. Nevertheless, the approach demonstrated to be vulnerable to geometric manipulations such as rotations.

II. Discrimination Test

In this test, we used the well-known structural similarity (SSIM) [22] for judging the ground truth. The SSIM is a widely used similarity metric for images. It compares two images and returns a score between 0 (no similarity) and 1 (full similarity). We compute the hash distance for about 1000 pairs of different images. The overall average hash distance is 0.4850. The average hash distances for some related methods are listed in Table II.

TABLE II: Average has Distance

Methods	Average block hash distance (standard deviation)
Ref 21	0.463
Ref 22	0.437
Proposed method	0.4850

III. Key Sensitivity

The chaotic signal is characterized by its sensitivity to initial conditions and the random-like behavior of chaotic signals in addition to their broadband spectrum, where it was believed that information could be hidden efficiently in chaos. So it is impossible to predict in the long term. This merit implies that two signals from the same chaotic systems with a slight change in initial conditions diverge with increasing time and will become uncorrelated signals with each other, as illustrated in Figure (8).

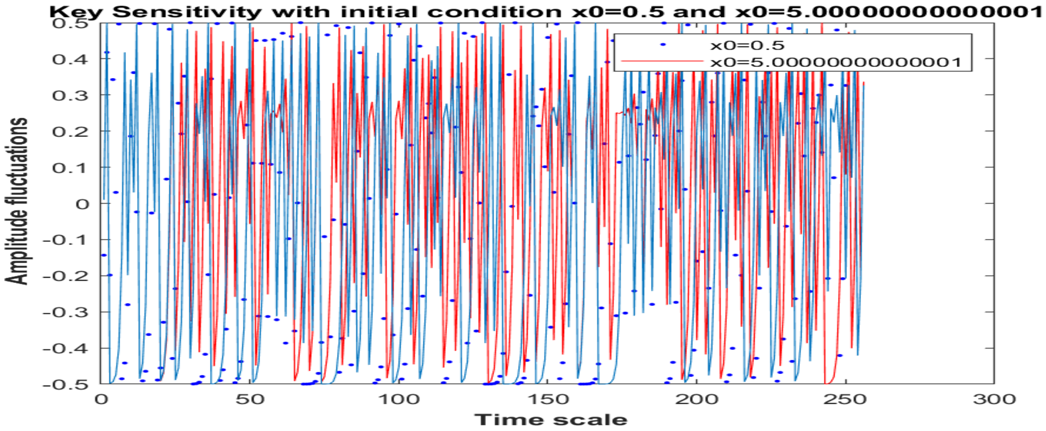


Figure 8: Chaotic signals are sensitive to initial conditions

From Figure 9, it is noticed that the Quadrate chaos generator exhibits good autocorrelation properties making a call for use in security applications. Figure 10 depicts the encoded hash after applying antipodal CSK, while Figure 11 depicts the cross-correlation between the encoded hash and the original hash.

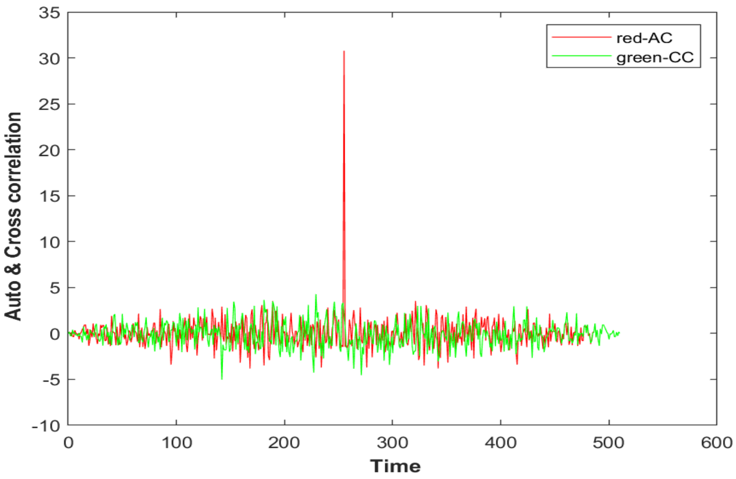


Figure 9: Auto and Cross-correlation performance for Quadrate map

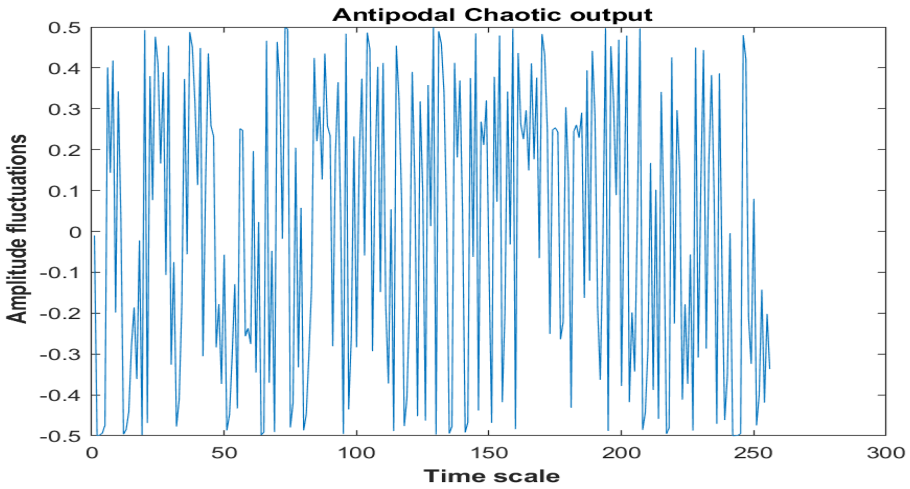


Figure 10: Encoded hash using antipodal CSK generator

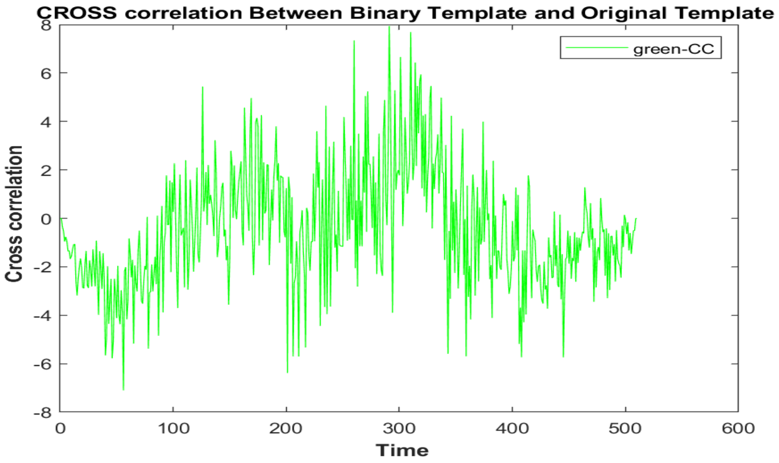


Figure 11: Cross-correlation between the coded template and the original template

From Figure 10 and Figure 11, it is noticed that the characteristics of outputs look like those of random Additive White Gaussian Noise (AWGN).

4. CONCLUSIONS

The concept of image hashing in the frequency domain with security supported by the CSK scheme is investigated. The feature set is extracted by integrated SLT and DCT transformations. This feature set is encrypted by a powerful chaotic map system. A detailed analysis was conducted using 1000 uncompressed images that were randomly chosen from a publicly available AANLIB database. The suggested method of security is ensured by the strength of the CSK and the encryption key secrecy. And the suggested hashing method was implemented well under filtering, Sharpening, and some geometric attacks compared with some related researches. The proposed hash scheme is applicable for image authentication.

References

[1] J. J. Ranjani , M. Babu, Medical Image Reliability Verification Using Hash Signatures and Sequential Square Encoding, J. Intell. Syst. 27(2018)19–30. https://doi.org/10.1515/jisys-2017-0019

[2]Y. Dai , X. Wang, Medical image encryption based on a composition of logistic maps and chebyshev maps, 2012 IEEE international conference on information and automation, (2012)210–214. **https://doi.org/**10.1109/ICInfA.2012.6246810

[3]A. B. Mahmood , R. D. Dony, Segmentation based encryption method for medical images, 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates ,(2011) 596–601.

[4] L. Laouamer, M. Al Shaikh, L. T. Nana, A. C. Pascu, Informed symmetric encryption algorithm for DICOM medical image based on N-grams, 2013 Science and Information Conference, London, UK (2013) 353–357.

[5] D. Bouslimi, G. Coatrieux, M. Cozic, C. Roux, A joint encryption/watermarking system for verifying the reliability of medical images, in IEEE Transactions on Information Technology in Biomedicine, 16(2012)891–899. https://doi.org/10.1109/TITB.2012.2207730

[6] A. K. Singh, M. Dave, A. Mohan, Hybrid technique for robust and imperceptible multiple watermarking using medical images, Multimed. Tools Appl., 75(2016)8381–8401. https://doi.org/10.1007/s11042-015-2754-7

[7] A. K. Singh, M. Dave, A. Mohan, Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain, Natl. Acad. Sci. Lett., 37(2014)351–358. https://doi.org/10.1007/s40009-014-0241-8

[8] B. Schneier, Applied cryptography: protocols, algorithms, and source code in *C*, john wiley & sons, 2007.

[9] L. Weng , B. Preneel, A secure perceptual hash algorithm for image content authentication, IFIP International Conference on Communications and Multimedia Security, 7025 (2011) 108–121. https://doi.org/10.1007/978-3-642-24712-5_9

[10] H. Huang, G. Coatrieux, H. Shu, L. Luo, C. Roux, Blind integrity verification of medical images, IEEE Trans. Inf. Technol. Biomed, 16(2012)1122–1126. https://doi.org/10.1109/TITB.2012.2207435

[11] V. Desai , D. H. Rao, Image Hash using Neural Networks, Int. J. Comput. Appl., 63(2013). https://doi.org/10.5120/10765-5578

[12] G. Coatrieux, H. Huang, H. Shu, L. Luo, C. Roux, A watermarking-based medical image integrity control system and an image moment signature for tampering characterization, IEEE J. Biomed. Heal. Informatics, 17(2013)1057–1067. doi:10.1109/JBHI.2013.2263533

[13] R. Eswaraiah , E. S. Reddy, Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest, IET Image Proc., 9(2015)615–625. https://doi.org/10.1049/iet-ipr.2014.0986

[14] P. T. Akkasaligar, S. Biradar, Medical Image Encryption with Integrity Using DNA and Chaotic Map, International Conference on Recent Trends in Image Processing and Pattern Recognition. (2019) 143–153. https://doi.org/10.1007/978-981-13-9184-2_13

[15] F. Ahmed, M. Y. Siyal, V. U. Abbas, A secure and robust hash-based scheme for image authentication, Signal Process., 90(2010)1456–1470. https://doi.org/10.1016/j.sigpro.2009.05.024

[16] A. T. Hashim , Z. A. Saleh, Visual Cryptography and CSK for Biometric Template Security, J. Eng. Appl. Sci., 13 (2018) 7642-7647. https://doi.org/10.36478/jeasci.2018.7642.7647

[17] G. A. Sathishkumar , K. Bhoopathy, N. Sriraam, Image encryption based on diffusion and multiple chaotic maps, Int. J. Net. Security Appl., 3 (2011)181-194. https://doi.org/10.5121/ijnsa.2011.3214

[18] K. A. Johnson, J. A. Becker, The Whole Brain Atlas. http://www.med.harvard.edu/AANLIB/ (accessed Nov. 18 2020).

[19] R. A. P. Hernandez, M. N. Miyatake, B. M. Kurkoski, Robust image hashing using image normalization and SVD decomposition, Conference Circuits and Systems, 2011 IEEE 54th International Midwest Symposium (2011). https://doi.org/10.1109/MWSCAS.2011.6026372

[20] S. S. Kozat, R. Venkatesan, M. K. Mihçak, Robust perceptual image hashing via matrix invariants, 2004 International Conference on Image Processing, 2004. ICIP'04., 5 (2004) 3443–3446. **https://doi.org/**10.1109/ICIP.2004.1421855

[21] R. L. Tataru, Image hashing secured with chaotic sequences, in 2014 Federated Conference on Computer Science and Information Systems, 2 (2014) 735–740. doi: http://dx.doi.org/10.15439/2014F250

[22] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, Image quality assessment: from error visibility to structural similarity, in IEEE Transactions on Image Processing. 13 (2004) 600 – 612. **https://doi.org/**10.1109/TIP.2003.819861