Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)

doi:10.3233/APC210171

An Image Encryption Technique Based on Logistic Sine Map and an Encrypted Image Retrieval Using DCT Frequency

Rajana Kanakaraju [a, 1], Lakshmi V [b], Shanmuk Srinivas Amiripalli [c], Sai Prasad Potharaju [d], R Chandrasekhar [b]

[a]*Department of Computer Science, Gayatri Vidya Parishad College for Degree and PG Courses, M.V.P Campus, Visakhapatnam, AP, India*

[b]*Department of Computer Applications, Gayatri Vidya Parishad College of Engineering(A), Madhurawada, Visakhapatnam, AP, India*

[c]*Dept of CSE, GITAM Univeristy, Visakhapatnam, AP, India*

[d]*Dept Computer Engineering, Sanjivani College of Engineering, Kopargaon, MH, India*

Abstract. In this digital era, most of the hospitals and medical labs are storing and sharing their medical data using third party cloud platforms for saving maintenance cost and storage and also to access data from anywhere. The cloud platform is not entirely a trusted party as the data is under the control of cloud service providers, which results in privacy leaks so that the data is to be encrypted while uploading into the cloud. The data can be used for diagnosis and analysis, for that the similar images to be retrieved as per the need of the doctor. In this paper, we propose an algorithm that uses discrete cosine transformation frequency and logistic sine map to encrypt an image, and the feature vector is computed on the encrypted image. The encrypted images are transferred to the cloud picture database, and feature vectors are uploaded to the feature database. Pearson's Correlation Coefficient is calculated on the feature vector and is used as a measure to retrieve similar images. From the investigation outcomes, we can get an inference that this algorithm can resist against predictable attacks and geometric attacks with strong robustness.

Keywords. Cloud Computing, confidentiality, encryption, decryption, feature vector, Pearson's correlation, discrete cosine transformation, image retrieval, logistic sine map.

1. Introduction

Nowadays, cloud computing technology is mostly used by many medical institutions to store medical data. Images occupy more space when compared to text messages and become a big issue if the data need to be shared, then the medical institutions are using

[1] Lakshmi V,Department of Computer Science, Gayatri Vidya Parishad College for Degree and PG Courses, Email: lakshmi.vkl@gvpce.ac.in.

untrusted third-party cloud platforms to store and share medical data, nevertheless Whenever the user stores their image data in the third-party cloud server, the users no Longer have the direct control over the data, which makes them tense about their privacy and confidentiality [1-4]. Thus, before storing data on the cloud server, the data should be converted into a not understandable manner. To encrypt images there are several approaches, the encryption algorithms in the spatial domain are instinctive and easy to implement and which makes use of the matrix structures of the image data, but due to high algorithm complexity and distortion of the image makes these encryption algorithms inefficient. In comparison, the encryption algorithms in the frequency domain are quite steady and can counterattack interfering. A combination of discrete cosine transformation and chaotic maps are used to encrypt images, there are many variants of chaotic maps, the most popular chaotic map used is logistic map but this map has lost its importance due to its drawbacks such as the non-uniform distribution of output sequences and the chaotic sequences exist only in a limited range, these drawbacks can be covered by another variant of a chaotic system called logistic sine map system which is a non-linear grouping of two different one dimensional chaotic maps [5].

To diagnose a disease, the doctor needs to do so much analysis. In some cases, the doctor uses medical images of past medical cases to do more precise diagnosis and also to take proper medical care. Hence, it is essential to have an effectual and operative medical image retrieval system. Old-style methods for retrieving similar images are meta search retrieval and image retrieval based off of content (CBIR), which mainly uses features as content, in particular text [6], color [7], composition, shape [8], and texture [9] as a feature vector. Feature vector plays a crucial role in image retrieval. However, the data in the cloud platform is encrypted, so that CBIR technology is not helpful in the image retrieval process as there is no use if the content is decrypted before retrieving and also increases a lot of unnecessary calculations. After a while, there is a novel and homomorphic encryption [10-12]. Homomorphism encryption is used in favor of doing arbitrary computations over the encrypted medical image data, with the identical outcome as the novel calculation of the original medical image [13-14].In the present study, we are proposing an algorithm for Encrypted Medical Image Retrieval which uses of Discrete Cosine Transformation (DCT) and Logistic Sine map. The algorithm uses DCT transformation with a Logistic sine map for encryption and uses Pearson's Correlation Coefficient between encrypted images to retrieve similar images [15-20]. The algorithm can resist against conventional and geometric attacks with strong robustness.

2. Preliminaries

Discrete Cosine Transform is used to translate the matrix data into a summation of a sequence of cosines fluctuating at different frequencies. It is like Discrete Fourier Transform (DFT), but discrete cosine transformation uses of just cosines and real coefficients. In contrast, Fourier transformation uses both cosines and sines and also requires complex number coefficients. Figure 1 Discrete cosine transformations simple to compute. Both discrete Fourier transform and discrete cosine transformation converts data into the frequency domain from a spatial domain, and the inverse

functions of DCT and DFT transform data into the original data. After the DCT transforms, the low-frequency part contains a highly concentrated attribute of energy and natural signals. The mathematical expressions for Forward DCT transformation and Inverse DCT transformation are as defined in Eq (1) and Eq (2) respectively. The pixel value in the frequency domain and spatial dominate represented by F(u, v) and f (x, y) respectively. The medical image size is represented by M and N. In Logistic Sine Maps Chaotic maps are highly used in image encryption because of their non-convergence, chaotic property, input sensitivity, and state ergodicity. The complex chaotic behavior is generated by using simple dynamic equations. The logistic sine map is a 1D chaotic map. It is a non-linear grouping 1D Logistic map and 1D Sine map. The equation to represent the Logistic Sine map, defined in equation (3). Where r is the input branch constraint with a scope of [0,4] and Xn is the chaotic output with a range of [0,1].

3. Proposed Algorithm

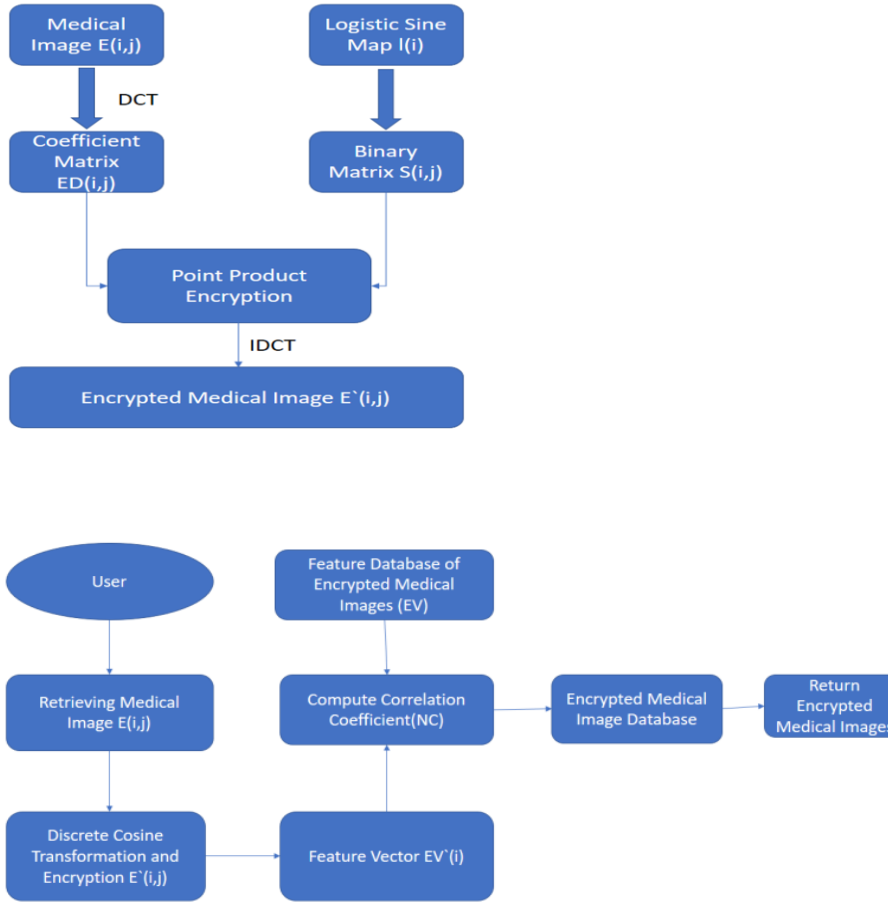

Figure 1. Phases of proposed model

Proposed Algorithm

Step1: *Initially, process the original medicinal image F (i, j) using DCT (Discrete Cosine Transformation), gaining a coefficient matrix of complex number i.e. FD (i, j);*
Step2: *Generate a 1D chaotic vector bl(j) by using logistic sine map after setting the initial value ofX0;*
Step3: *Create a binary matrix S(i,j) which consists of -1 and 1. The 1D chaotic vector bl(j) is used to construct a binary matrix by using a threshold routine sign(l).*

Step4: *Then, do dot product between binary matrix S(i,j) and the complex matrix FD(i,j) which outputs a matrix L(i,j);*

Step5: *To acquire an encrypted image E(i,j), the L(i,j) is processed using IDCT (Inverse Discrete Cosine Transformation).*

Step6: *At first the encrypted image E(i,j) is processed using DCT, then attaining a complex number matrix ED(i,j);*

Step7: *Consider ED``(i,j) upper left corner's 8 X 8 low frequency matrix of ED(i,j),: By using a sign function, create a binary sequence that consists of 1's and 0'sas a feature vector from step2.*

Step 8. *The features FV={FV1, FV2…, FVN} are calculated for encrypted images in the encrypted database E={E1, E2…, EN}.and Upload FV={FV1,FV2…,FVN} into feature database.*
Step 9: *Encrypt the medical image E (i,j) which is uploaded by user, results in an encrypted image E`(i,j) and Extract feature vector FV`(j) for encrypted medical image E`(i,j);*

Step 10: *Calculate Cross-Correlation between FV`(j) and feature vectors in feature database FV(j) using the equation (9) and Retrieve the encrypted medical image, which has the maximum Cross-Correlation value (Near to 1.0)Where mx is the mean of the vector x and my is the mean of the vector y.*

4. Results and Discussion

In this study, the model used for simulation is Python 3.7, we pick the MRI information, and the motivation behind the analysis is to examine the algorithm under various attacks and to test whether the retrieval algorithm is retrieving the images or not and also to prove the robustness and homomorphism of the algorithm The outcomes of the experiments are as follows To demonstrate that the feature obtained by the technique mentioned in this paper is a significant feature of the encrypted image. We conducted experimentations among various medical images (made known in figure 2) and their encrypted images (made known in figure 3). By noticing table 1 to table 7 it can be found that the higher the correlation value, higher the similarity, and lower the

correlation value, lower the similarity. It also found that the correlation value between the original medical image and the decrypted medical image is also 1.0 so that the encryption algorithm is lossless and also found that the encryption algorithm is maintaining homomorphic features. Peak Signal to Noise Ratio (PSNR) is broadly used to assess the quality of the picture. In this study, we use PSNR to impartially assess the quality of the picture to be retrieved after the attacks. An experiment is conducted to retrieve encrypted medical images from cloud platforms by passing a medical image to the system.

The system retrieved the images which are having a cross-correlation value of less than 0.5, and then the results obtained are as follows. To prove that the algorithm is retrieving encrypted images even in interference of Gaussian noise, we did experiments on images by increasing the intensity of Gaussian noise to an image. The algorithm has strong anti-Gaussian ability as the image is retrieved even with Gaussian intensity of 20% and the cross-correlation value is 0.86. The results of the experiment are as follows. To prove that the algorithm is retrieving encrypted images against JPEG compression attacks, the experiments were conducted on a medical image while compressing the image up to 50%. The results proved that the algorithm is good enough against the JPEG compression attacks and the results are as follows. The research on median filtering attacks was conducted on a medical image by altering the median filter size and by the number of repeats.

The results have shown that the algorithm has strong sturdiness against median filter assaults. The experiments are conducted up to a size of 3 x3 to 7 x 7. The results of the experiments concluded that the algorithm is strong enough to handle rotation attacks. The experiment goes through various rotations of the image, the retrieval system successfully retrieved the images which are rotated up to 10o. The algorithm has undergone various experiments and proved that it is durable against scaling attacks as the experimental results proved that the retrieval system was successfully retrieved images even with a scaling factor between 0.2 and 4.0. The investigation outcomes proved that the algorithm is tough against cropping attacks and the cropping has done against the medical image on both x and y axes. The cropping ratio for each axis is from 2 % to 20.

Table 1. Cross-correlation between the feature and vector of different encrypted medical images

	a	**b**	**C**	**d**	**e**		**Ea**	**Eb**	**Ec**	**Ed**	**Ee**
a	1.0	0.26	0.03	0.05	-0.12	**Ea**	1.0	0.19	0.09	0.13	-0.03
b	0.26	1.0	0.35	0.07	-0.29	**Eb**	0.19	1.0	0.41	-0.12	0.03
c	0.03	0.35	1.0	-0.09	0.06	**Ec**	0.09	0.41	1.0	-0.28	0.06
d	0.05	0.07	-0.09	1.0	-0.09	**Ed**	0.13	-0.12	-0.28	1.0	-0.03
e	-0.12	-0.29	0.06	-0.09	1.0	**Ee**	-0.03	0.03	0.06	-0.03	1.0

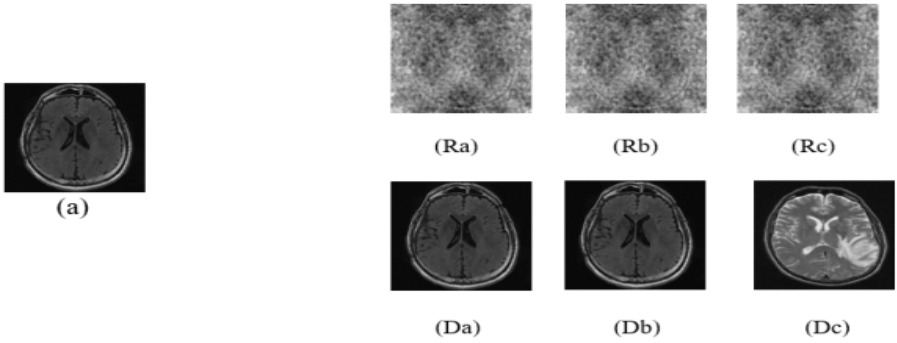

Figure 2. (a) Medical Images (b) Retrieved encrypted medical images (c) decrypted retrieved medical images

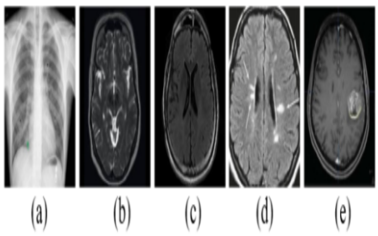

Figure 3. a Medical Images

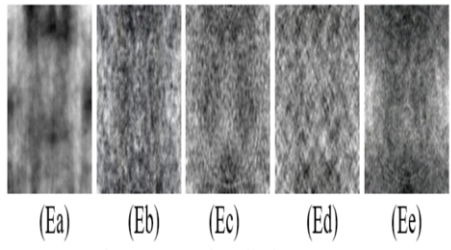

Figure 3. b Encrypted Medical Images

Table 2. Experimental results of Gaussian noise

Noise Intensity	1	4	6	8	12	16	20
PSNR (dB)	21.33	16.64	14.86	13.62	12.91	11.31	10.06
Cross Correlation	0.98	0.95	0.92	0.91	0.89	0.88	0.86

Table 3. Experimental results of JPEG compression attacks

Percentage (%)	5	12	17	22	27	35	42	50
PSNR (dB)	21.22	24.67	25.55	26.56	26.80	27.67	27.73	28.58
Cross Correlation	0.98	0.98	0.97	0.98	0.98	0.98	0.98	0.98

Table 4. Experimental results of median filtering attacks

	Size of Median Filter								
	[3 x 3]			[5 x 5]			[7 x 7]		
Repeating times	2	5	10	2	5	10	2	5	10
PSNR (dB)	28.41	27.46	25.85	25.55	24.71	22.50	23.99	24.32	21.23
Cross Correlation	1.0	1.0	1.0	1.0	0.93	0.90	0.93	0.93	0.85

Table 5. Experimental results of rotation attacks

Degree (o)	-10o	-5o	-1o	0o	1o	5o	10o
PSNR (dB)	14.16	16.01	22.79	103.49	22.80	16.14	14.18
Cross Correlation	0.60	0.74	0.92	1.0	0.90	0.75	0.50

Table 6. Experimental results of rotation attacks

	Ratio (%)	2	4	6	8	10	12	14	16	18	20
X	Cross-Correlation	0.81	0.79	0.78	0.70	0.63	0.47	0.47	0.44	0.37	0.44
Y	Cross-Correlation	0.91	0.84	0.75	0.75	0.79	0.78	0.62	0.59	0.59	0.56

Table 7. Experimental results of scaling attacks

Scaling Factor	0.2	0.4	0.6	1.00	1.2	1.5	2.0	4.0
Cross Correlation	0.75	0.97	0.97	1.00	1.00	1.00	1.00	1.00

5. Conclusion

In this research paper a strong algorithm to retrieve encrypted images is proposed, which is a combination of logistic sine map, 2D discrete cosine transform, and feature extraction in the encrypted field. The investigational efforts demonstrate that this algorithm has perfect sturdiness against Median filtering, cropping attacks, Rotation attacks, Gaussian noise, JPEG compression and scaling attacks. This algorithm is also used to secure medical image data. Moreover, this algorithm has a fast retrieve speed and good operability.

References

[1] Xia, Z., Xiong, N. N., Vasilakos, A. V., & Sun, X. (2017). EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing. Information Sciences, 387, 195-204.

[2] Index, G. W. (2013). Instagram tops the list of social network growth.

[3] Ferretti, L., Pierazzi, F., Colajanni, M., & Marchetti, M. (2013, August). Security and confidentiality solutions for public cloud database services. In The Seventh International Conference on Emerging Security Information, Systems and Technologies (pp. 36-42).

[4] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[5] Zhou, Y., Bao, L., & Chen, C. P. (2014). A new 1D chaotic system for image encryption. Signal processing, 97, 172-182.

[6] Simpson, M. S., You, D., Rahman, M. M., Xue, Z., Demner-Fushman, D., Antani, S., & Thoma, G. (2015). Literature-based biomedical image classification and retrieval. Computerized Medical Imaging and Graphics, 39, 3-13.

[7] Chatzichristofis, S. A., & Boutalis, Y. S. (2008, May). CEDD: Color and edge directivity descriptor: A compact descriptor for image indexing and retrieval. In International conference on computer vision systems (pp. 312-322). Springer, Berlin, Heidelberg.

[8] Potharaju, S. P., Sreedevi, M., & Amiripalli, S. S. (2019). An Ensemble Feature Selection Framework of Sonar Targets Using Symmetrical Uncertainty and Multi-Layer Perceptron (SU-MLP). In Cognitive Informatics and Soft Computing (pp. 247-256). Springer, Singapore.

[9] Vo, A., & Oraintara, S. (2010). A study of relative phase in complex wavelet domain: Property, statistics and applications in texture image retrieval and segmentation. Signal Processing: Image Communication, 25(1), 28-46.
[10] Marwan, M., Kartit, A., & Ouahmane, H. (2016, October). Applying homomorphic encryption for securing cloud database. In 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt) (pp. 658-664). IEEE.
[11] Liu, J., Han, J. L., & Wang, Z. L. (2016, July). Searchable encryption scheme on the cloud via fully homomorphic encryption. In 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC) (pp. 108-111). IEEE.
[12] Xu, Y., Gong, J., Xiong, L., Xu, Z., Wang, J., & Shi, Y. Q. (2017). A privacy-preserving content-based image retrieval method in cloud environment. Journal of Visual Communication and Image Representation, 43, 164-172.
[13] Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. Foundations of secure computation, 4(11), 169-180.
[14] Potharaju, S. P., & Sreedevi, M. (2018). A novel cluster of quarter feature selection based on symmetrical uncertainty. Gazi University Journal of Science, 31(2), 456-470.
[15] Zhang, C., Li, J., Wang, S., & Wang, Z. (2017, June). An encrypted medical image retrieval algorithm based on DWT-DCT frequency domain. In 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA) (pp. 135-141). IEEE.
[16] Naidu, J. L., Gorakala, A. C., & Amiripalli, S. S. (2020). Hash functions and its security for Snags.
[17] Amiripalli, S. S., & Bobba, V. (2019). An Optimal TGO Topology Method for a Scalable and Survivable Network in IOT Communication Technology. Wireless Personal Communications, 107(2), 1019-1040.
[18] Amiripalli, S. S., & Bobba, V. (2019). Impact of trimet graph optimization topology on scalable networks. Journal of Intelligent & Fuzzy Systems, 36(3), 2431-2442.
[19] Jitendra, M. S., Amiripalli, S. S., Kollu, V. V. R., Chowdary, P. R., & Rao, R. V. (2020). Analysis of Airline Connectivity System using Graph Theory. International Journal of Control and Automation, 13(4), 77-84.
[20] Amiripalli, S. S., Kumar, A. K., & Tulasi, B. (2016, February). Introduction to TRIMET along with its properties and scope. In AIP Conference Proceedings (Vol. 1705, No. 1, p. 020032). AIP Publishing LLC.