A Robust Chaos-Based Technique for Medical Image Encryption

Dr.P.Pandi selvi, Ms.S.Lakshmi Priya
Assistant Professor, Department of Computer Science, Mangayarkarasi College of Arts and Science for Women, Paravai, Madurai
PG Student, Mangayarkarasi College of Arts and Science for Women, Paravai, Madurai

Abstract: Medical images possess significant importance in diagnostics when it comes to healthcare systems. These images contain confidential and sensitive information such as patients' X-rays, ultrasounds, computed tomography scans, brain images, and magnetic resonance imaging. However, the low security of communication channels and the loopholes in storage systems of hospitals or medical centres put these images at risk of being accessed by unauthorized users who illegally exploit them for non-diagnostic purposes. In addition to improving the security of communication channels and storage systems, image encryption is a popular strategy adopted to ensure the safety of medical images against unauthorized access. In this work, the authors propose a lightweight cryptosystem based on Henon chaotic map, Brownian motion, and Chen's chaotic system to encrypt medical images with elevated security. The effciency of the proposed system is proved in terms of histogram analysis, adjacent pixels correlation analysis, contrast analysis, homogeneity analysis, energy analysis, NIST analysis, mean square error, information entropy, number of pixels changing rate, unifed average changing intensity, peak to signal noise ratio and time complexity. The experimental results show that the proposed cryptosystem is a lightweight approach that can achieve the desired security level for encrypting confidential image-based patients' information.

INTRODUCTION

Image steganography comprises of transform domain, model relied steganography, spatial domain and spread spectrum. The spatial domain and transform domain contrasts with one another. Pixel value is directly used to embed a secret message in spatial domain. On the other hand, transform domain techniques accomplish embedding by initially transforming the particular image from STF (Spatial to Frequency) domain via the use of any of the mentioned transforms. They are DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform), Ridge let Transform, Hadamard Transform, DD DT DWT (Double Density Dual Tree DWT). The recent progress in the communication and information technology generates easy and simple accessible data. The steganography is used for data transfer over multi-media transfers such as image, video, audio and so on. Thus, steganography means "hidden-data". This is derived from greek word "steganographia". This word integrates the two words "steganos" and "graphia". This reveals that this particular methodology has been used from ancient period. Through this technique, the data is sent from sender to the receiver without any malicious activity and thirdparty interruption. Additionally, the data is trustworthy and consistent during the transfer by the use of this data hiding methodology.

LITERATURE SURVEY

In 2017, Saleh Delbarpour Ahmadi,et al, Selects a block of the host image and then employs AIS for finding the best template for embedding message bits in the host image pixels. Consequently, their method finds the best template for embedding rapidly and there is no need to investigate whole image for finding a template of embedding. Algorithm has more efficiency in term of embedding capacity and the time of the embedding process, when compared to other methods

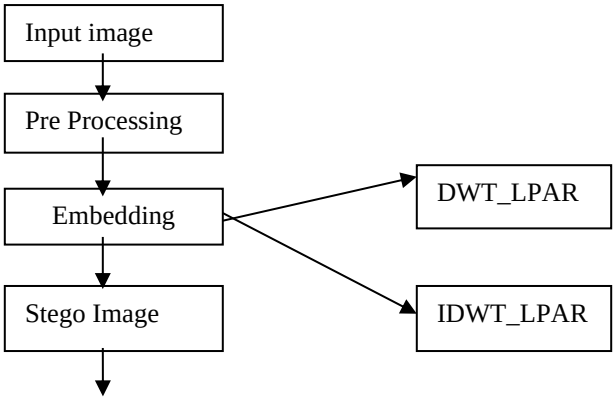
In 2018, de rosal ignatius moses setiadi et al, aimed to make confidential information more secure and inaccessible to unauthorized persons by coupling Steganography domains with Cryptography. Messages that are encrypted using the 3-DES side of the cover image was decomposed into using LSB

method. Their last step, done Inverse DWT (IDWT) to get the stego image.

In 2018, ahmed hambouz et al**,** introduced a new steganography technique that achieves both data confidentiality and integrity. Data confidentiality is achieved by embedding the data bits in a secret manner into stego image. Integrity is achieved using SHA 256 hashing algorithm to hash the decoding and encoding variables.

In 2020, songul karakus et al, introduced a method to improvise, data hiding capacity and image quality of the cover object in image steganography. The main reason is that the deterioration of image quality can be noticed by the human vision system, as it attracts the attention of attackers. Therefore, the purpose of their study is increasing the amount of data to be hidden and stego image is to ensure high image quality.

METHODOLOGY



Input Data:

The data selection is the process of selecting and loading the input images from the dataset. The dataset is used to Segregate the image from the input Image. The given image is read with the imread() function.

Pre-processing:

Once after importing the input image, it needs to be preprocessed. It is carried out by resizing the image and removing any noise present in the image.

DWT_LPAR:

DWT is a wavelet transform for which the wavelets are sampled at discrete intervals. DWT provides simultaneous spatial and frequency domain information of the image. In DWT operation, an image can be analyzed by the combination of analysis filter bank and decimation operation. Discrete Wavelet transform (DWT) is used as a feature extraction because it is a powerful tool of signal processing because of it's multiresolutional possibilities. The chosen data is encrypted with one of conventional cryptographic algorithm.

Extract the Hidden Data:

It is necessary to extract the hidden information from the given input image. It affords stego images which consists of hidden data, yet seems to have more visual fidelity.

Performance Analysis:

The final result gets generated based on the overall prediction. The performance of the proposed approach is evaluated using measures like,

- Accuracy
- Precision
- Recall
- F1-Score

RESULT AND DISCUSSION

Final Result gets generated based on the overall performance of the proposed approach as it is evaluated using some measures like:

PSNR

Peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible power of an image and the power of corrupting noise that affects the quality of its representation**.**

MSE

MSE is used to check how close estimates or forecasts are to actual values. Lower the MSE, the closer is forecast to actual. This is used as a model evaluation measure for regression models and the lower value indicates a better fit**.**

The output of the proposed system is as shown in the below figure 1.

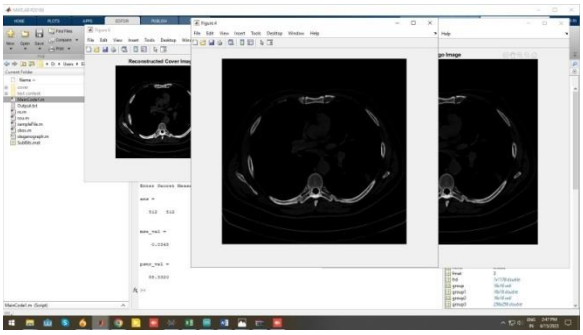


Figure 1: Output of the proposed system

CONCLUSION

In order to achieve the desired level of security in storage systems of hospitals and medical centers. The proposed system achieves confusion through two-dimensional Henon chaotic map (HCM), whereas difusion is obtained using BM and CCS. Furthermore, the reliability and security of the proposed system are analyzed and compared with existing techniques using the following parameters. The NIST and entropy measures are obtained through randomness test, the consistency and variance through histogram examination, and the pixel similarity using a coefficient of correlation. Other performance analysis parameters include energy, contrast, homogeneity, mean square error, peak to signal noise ratio, number of pixels changing the rate, unified average changing intensity, and computational complexity. The results show that the proposed system outperforms existing image encryption systems in terms of higher security. In addition, the proposed system requires less computational resources and, at the same time, offers fast processing making it suitable for application in real-time encryption. As a future direction, the proposed encryption scheme can be modified in order to encrypt other media formats including audio and video.

REFERENCE

[1] S. D. Ahmadi and H. Sajedi, "Image steganography with artificial immune system," in 2017 Artificial Intelligence and Robotics (IRANOPEN), 2017, pp. 45-50.

[2] G. Ardiansyah, C. A. Sari, and E. H. Rachmawanto, "Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm," in 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017, pp. 249-254.

[3] A. Hambouz, Y. Shaheen, A. Manna, M. Al-Fayoumi, and S. Tedmori, "Achieving Data Integrity and Confidentiality Using Image Steganography and Hashing Techniques," in 2019 2nd International Conference on new Trends in Computing Sciences (I)

[4] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018.

[5] S. Karakus and E. Avcı, "A New Image Steganography Method wıth Optımum Pıxel Sımılarıty for Data Hıdıng ın Medıcal Images," Medical Hypotheses, p. 109691, 2020.

[6] M. Kaur and M. Juneja, "A new LSB embedding for 24-bit pixel using multi-layered bitwise XOR," in 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, pp. 1-5.

[7] J. Kim, H. Park, and J.-I. Park, "CNN-based image steganalysis using additional data embedding," Multimedia Tools and Applications, vol. 79, pp. 1355-1372, 2020.

[8] L. Laimeche, A. Meraoumia, and H. Bendjenna, "Enhancing LSB embedding schemes using chaotic maps systems," Neural Computing and Applications, pp. 1-19, 2019.

[9] N. A. Loan, S. A. Parah, J. A. Sheikh, J. A. Akhoon, and G. M. Bhat, "Hiding electronic patient record (epr) in medical images: A high capacity and computationally efficient technique for e-healthcare applications," Journal of biomedical informatics, vol. 73, pp. 125-136, 2017.

[10] A. Miri and K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm," Optik, vol. 145, pp. 158-168, 2017.8

[11] S. Nipanikar, V. H. Deepthi, and N. Kulkarni, "A sparse representation based image steganography using particle swarm optimization and wavelet transform," Alexandria engineering journal, vol. 57, pp. 2343-2356, 2018.

[12] S. A. Parah, J. A. Sheikh, J. A. Akhoon, and N. A. Loan, "Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," Future Generation Computer Systems, vol. 108, pp. 935-949, 2020.

[13] P. Rahmani and G. Dastghaibyfard, "An efficient histogram-based index mapping mechanism for

reversible data hiding in VQ-compressed images," Information Sciences, vol. 435, pp. 224-239, 2018.
[14] C. Y. Roy and M. K. Goel, "Visual Cryptographic Steganography with Data Integrity," Lovely Professional University, 2017.
[15] K. Sakthidasan and N. V. Nagappan, "Noise free image restoration using hybrid filter with adaptive genetic algorithm," Computers & Electrical Engineering, vol. 54, pp. 382-392, 2016.
[16] D. K. Sarmah and A. J. Kulkarni, "Improved cohort intelligence—a high capacity, swift and secure approach on JPEG image steganography," Journal of information security and applications, vol. 45, pp. 90-106, 2019.
[17] A. K. Sahu and G. Swain, "A review on LSB substitution and PVD based image steganography techniques," Indonesian Journal of Electrical Engineering and Computer Science, vol. 2, pp. 712-719, 2016.
[18] K.Sreehari and R. Bhakthavatchalu, "Implementation of hybrid cryptosystem using DES and MD5," in 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018, pp. 52-55.
[19] M. Umair, "Comparison of Symmetric Block Encryption Algorithms," ResearchGate, 2017.