A Reversible Data Hiding Algorithm for Secured E-Healthcare Applications

Anasua Choudhury, Harsh Vardhan Chaudhry and Arkyajyoti Saha|Prof. Thanikaiselvan V. | SENSE

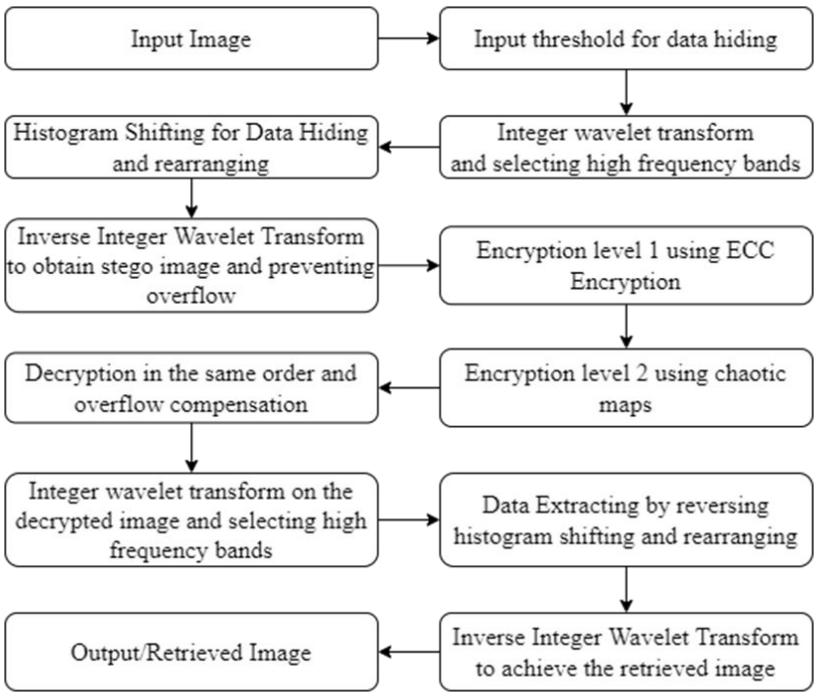
Motivation/ Introduction

The role of telemedicine in healthcare is growing everyday with thousands of digital operations across the field to make Healthcare efficient, accessible and secure. One such digitalized operation in the domain is the communication of patient information electronically. This comes with the evergreen threat of middle-men and hackers who can steal this information or tamper with it. With an increase in accessibility of telediagnosis for patients, the emphasis has been brought on the secure communication of patient image or text-based reports to its various remote centers. This makes the access to a secure means of patient data communication essential to the e-healthcare framework.

SCOPE of the Project

The project objective is to create a strong image encryption and data hiding algorithm against the backdrop of an e-healthcare framework which is one of the most vital parts of our digitalized economy. The proposed algorithm employs an Integer Wavelet Transform (IWT) and Elliptic Curve Cryptography (ECC) based asymmetric key hill cipher approach and chaotic maps for encryption of the medical images and a histogram-shift based reversible data hiding for secure transmission of the medical images. The patient data is decomposed using IWT before encryption using the ECC key hill cipher algorithm for first level of encryption and chaotic maps for the second level of encryption. The data transmission is them hidden using histogram-shift based approach before recovery at end point.

Methodology



Input Image

Input threshold for data hiding

Integer wavelet transform and selecting high frequency bands

Histogram Shifting for Data Hiding and rearranging

Inverse Integer Wavelet Transform to obtain stego image and preventing overflow

Encryption level 1 using ECC Encryption

Encryption level 2 using chaotic maps

Decryption in the same order and overflow compensation

Integer wavelet transform on the decrypted image and selecting high frequency bands

Data Extracting by reversing histogram shifting and rearranging

Inverse Integer Wavelet Transform to achieve the retrieved image

Output/Retrieved Image

Figure 1

Elliptic Curve Cryptography (ECC)

As the name recommends, ECC is an asymmetric cryptography method in light of uses of the mathematical construction of elliptic curves over finite fields. The mathematical construction satisfies the following equation:

$$y^2 = x^3 + ax + b$$

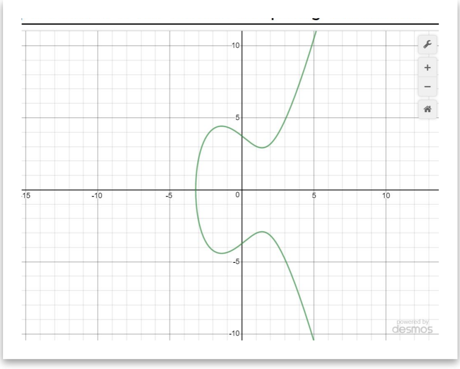


Figure 2

Integer Wavelet Transform (IWT)

The IWT is an invertible integer-to-integer wavelet analysis method. IWT can be used in your desired applications to deliver integer coefficients for integer-encoded signals. Contrasted and the continuous wavelet transform (CWT) and the discrete wavelet transform (DWT), the IWT isn't just computationally quicker and more memory-proficient yet additionally more suitable in lossless data-compression applications. The IWT empowers you to reproduce an integer signal impeccably from the computed integer coefficients.

Chaotic Maps

A chaotic map is a map (namely, an evolution function) that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter. Discrete maps usually take the form of iterated functions. Chaotic maps often occur in the study of dynamical systems. Of some kind. Guides might be defined by a discrete-time or a ceaseless time boundary.

Results

Histogram Analysis:

Figure 3: Lena test Image

(A)

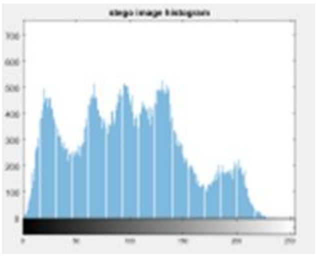


Figure 4

(B)

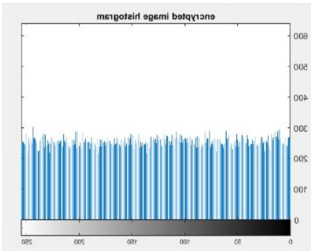


Figure 5

(C)

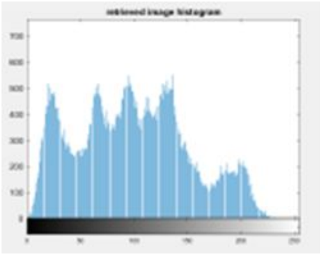


Figure 6

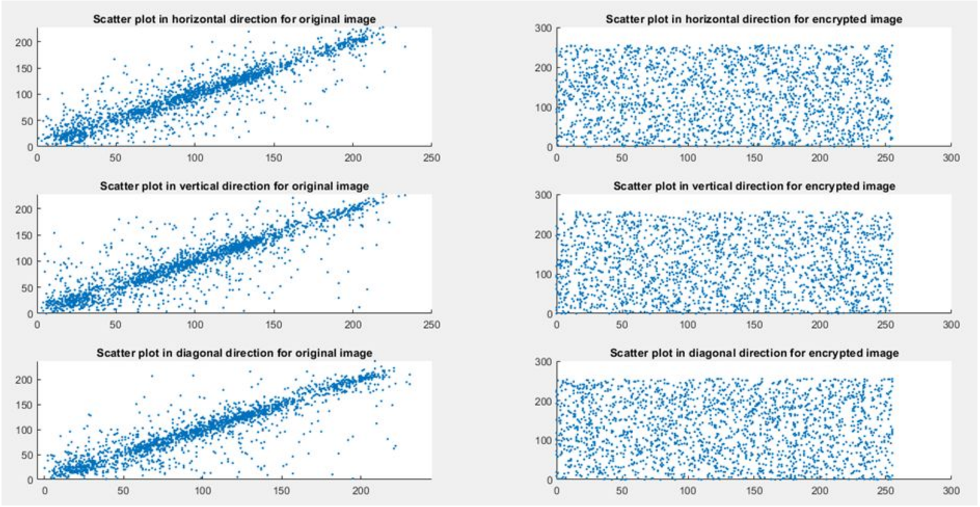


Figure 7

Table 1

Test Images	Correlation Coefficient					
	Horizontal Direction		Vertical Direction		Diagonal Direction	
	Original Image	Encrypted Image	Original Image	Encrypted Image	Original Image	Encrypted Image
Lena.jpg	0.9231	0.0418	0.8997	0.0076	0.9109	0.0014
Boat.jpg	0.8902	0.0383	0.8379	0.0281	0.8639	0.0143
Bridge.jpg	0.9054	0.0101	0.8257	0.0119	0.8301	0.0136
Lighthouse.jpg	0.7735	-0.0072	0.6775	-0.032	0.6832	-0.0014
Baboon.bmp	0.7995	-0.0154	0.7524	-0.0211	0.7240	-0.0357
Hill.png	0.9222	0.0058	0.8874	0.0085	0.8866	-0.0084
Einstein.png	0.9141	0.0032	0.8706	0.0282	0.8891	-0.0300
Cameraman.gif	0.8971	-9.5737e-04	0.8894	-0.0262	0.8855	0.0104

Table 2

NPCR (%)	UACI (%)
99.62	30.5657
99.63	28.3217
99.63	29.9265
99.62	29.9665
99.62	31.9283
99.63	29.3672
99.62	28.8745
99.62	35.1664

Conclusion/ Summary

The proposed algorithm has been carried out and its performance has been measured and verified against performance measures such as entropy, NPCR, UACI and Correlation coefficient of the pixels in different directions for various cases. This was performed on 8 such images and the results were recorded and compared with each other and the various parameters as mentioned. We concluded a satisfactory and reliable RDH algorithm that can be put to use on medical images for ensured security during transmission.

Contact Details:

Anasua Choudhury	18BEC0694	anasuachoudhury14@gmail.com
Harsh Vardhan Chaudhry	18BEC2035	
Arkyajyoti Saha	18BEC0938	

Acknowledgments/ References

[1] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari and Wei Su, IEEE Transactions on Circuits And Systems for Video Technology, Vol. 16, No. 3, March 2006

[2] Ambika Oad, Himanshu Yadav and Anurag Jain, A Review: Image Encryption Techniques and its Terminologies, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014

[3] Prasenjit Kumar Das, Mr. Pradeep Kumar and Manubolu Sreenivasulu, Image Cryptography: A Survey towards its Growth, Advance in Electronic and Electric Engineering. ISSN 2231-1297, Volume 4, Number 2 (2014), pp. 179-184, Research India Publications