Fast Efficient Transforms for Contour Extraction from Encrypted Medical Image

Ali abdrhman Ukasha[1*], Ali Ahmed Ganoun[2]

[1] ali.ukasha@sebhau.edu.ly, [2] ali.ganoun@ee.edu.ly

[1] Department of Electrical & Electronics Engineering, Faculty of Engineering & Technology Sciences, Sebha University, Libya
[2] Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Tripoli, Libya

*Corresponding author email: ali.ukasha@sebhau.edu.ly
Received: 00 April 2018 / Accepted: 00 May 2018

A B S T R A C T

The necessity of knowing the boundaries of the image is occupies the most important to researchers. With clear conrours, the doctor can easily diagnose the patient's condition. This is possible, but the challenge is whether we can do that for the medical image after it has been encrypted. The encryption algorithm used here is Rivest-Shamir-Adleman (RSA) algorithm which uses two-key encryption, one of them is secret. In this work we introduce a new idea to extract the contours from the encrypted image after converting them to spectral domain methods using Lifting Wavelet, Walsh, and Periodic Haar Piecewise-Linear Transforms. In the specrum image, the compression is done using zonal sampling method. To increase security, the Arnold transform will be applied to the encrypted image using privat keys. The contours extraction from the reconstructed medical image can performed using Canny edge detector. The comparison between those specral algorithms is performed in terms of energy retained, consumed time, compression ratio, and the contour points number which can be detected by the edge detector operator. The experiments results show that by this algorithm, the high number of contour points can be easily detected from the transmitted encrypted medical image and is better using DCT transform for the same compression ratio. However the higher compression ratio using PHL transform is obtained and is exceeds to 88.5391% with retained energy reached to 84.125%.

Keywords: RSA Encryption, Lifting Wavelet Transform, PHL Transform, DCT and Walsh Transforms, Contour Extraction, Canny Edge Detectors.

1 Introduction

The field of cryptography now encompasses much more than secret communication, including message authentication, digital signatures, protocols for exchanging secret keys, authentication

protocols, electronic auctions and elections, and digital cash [1]. According to the type of keys used for encryption (ke), respectively for decryption (kd), the cryptosystems are symmetric (private key) or asymmetric (public key). It is hard to overestimate the importance of public key cryptosystems and their associated digital signature schemes in the modern world of computers and the Internet [2].

There is a process exist that are used for sending information in secret way. This process is known as cryptography [3]. This paper will highlight a new method that is developed for more security where image can be encrypted by using cryptography [4]. In the present paper, RSA (Rivest, Shamir, and Adleman) in 1978, are used for image encryption.

2 Lifting Scheme of Wavelet Transform

In this work, we present the medical image contours compression processor with configurable lossy compression based on by taking advantage of the integer-to-integer lifting wavelet transform (LWT) via Haar wavelet [5]. LWT is characterized by simplicity, on location processing, and filter similarity. It provides low computational process in compare with filter banks used in regular Discrete Wavelet Transform (DWT). LWT is applied by three major steps [5][6]: Split: Split step also called the lazy wavelet, where the signal is being separated into smaller subsets. Generally, coefficients are divided into odd and even samples. Predict: Even samples are used to predict the odd ones, pixel at odd position are predicted by its two neighbours at even positions, then the difference between the predicted value and real odd value is stored in the location of odd samples. Signal after prediction step is the details band. Update: However, due to the nonlinearity changing in image pixels, even samples interposed the odd ones cannot be taken directly as they need to be "Updated" with the differences computed in predict steps (2). Inverse of lifting scheme is performed by reversing the order and exchanging the sign of predict and update steps [6]. In addition, the lifting approaches need 50% less computation than wavelet transform based FIR filters, subsequently the memory requirements is reduced. Lifting scheme was adopted by JPEG 2000 due to these properties [7].

3 Periodic Haar Piecewise-Linear (PHL) Transform

The set of N Haar functions is defined by [9]:

The set of periodic Haar piecewise linear functions are determined by:

$$\mathrm{PHL}(o,t) = 1, \qquad t \in (-\infty, \infty) \tag{1}$$

$$\mathrm{PHL}(1,t) = \left[\frac{2}{T}\int_{mT}^{t+mT} har(1,\tau)\,d\tau\right] + \frac{1}{2}, \quad \mathrm{PHL}(i+1,t) = \frac{2^{k+1}}{T}\int_{mT}^{t+mT} har(i+1,\tau)\,d\tau \tag{2}$$

where:

$i = 1,2,\ldots, N\text{-}2; \quad k = 1,2,\ldots, (\log_2 N)\text{-}1; \qquad m = 0,1,2,\ldots$

k – index of group of PHL functions

m – number of period.

The normalization factor (2^{k+1}) is applied to normalize the maximum amplitude of the PHL functions. The set of PHL functions is linearly independent but not orthogonal.

4 Discrete Cosine Transform (DCT)

Discrete Cosine Transform converts the signal into its elementary frequency components. After applying DCT, most of the energy of a signal is concentrated into top left corner of an image. Due to this property, DCT is widely used in image compression.
For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT. The lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion.

5 Fast Walsh Transform (FWT)

Walsh-Hadamard transform is powerful in a variety of applications in image and video coding, speech processing, data compression, communications [10, 11]. The fast Walsh-Hadamard transform algorithm generally applies to Hadamard matrices. The sequency ordering of the rows of the Walsh matrix can be derived from the ordering of the Hadamard matrix by first applying the bit-reversal permutation and then the Gray code permutation. The 2X2 Hadamard matrix is defined as H_2 is given in equation (3)

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{3}$$

The fast walsh-hadamard transform (FWHT) is utilized to obtain the local structure of the images. This basis function can be effectively used to obtain the digital numbers in the sense of coefficients [12] [13]. The implementation of FWHT readily reduces the time consumption for medical image registration when comparing the same with conventional WT technique for image registration. The simplicity of Walsh transform intrigued research efforts in cryptanalytic techniques for symmetric crypto-systems two decades ago [14].

6 RSA (Rivest-Shamir-Adleman)

RSA is an asymmetric system, which means that a key pair will be generated, a public key and a private key, obviously you keep your private key secure and pass around the public one. The

algorithm was published in the 70's by Ron Rivest, Adi Shamir, and Leonard Adleman (RSA). Strong security of multimedia data against attacks has been ever-increasing in order to protect confidentiality and integrity of sensitive data against attackers. RSA is one of the most popular and secure public key cryptosystems. It is normally considered as a strong asymmetric key cryptographic technique. The foundation of RSA's security relies upon the fact that determining the prime factors of a composite number is a hard process [15], [16]. The initial seed of RSA keys is the product of two prime numbers. Encoding and decoding keys have an exponential expressions and the cipher text size depending on the key size [15]. So, intricacy of breaking the algorithm is augments when size of prime numbers enlarges [17].
Many application areas used RSA including: secure data transmission browser security, the secure exchange of session keys on internet, internet banking, and credit card payments, smart cards, secure storage of secret keys [16], [17].

7 The Proposed Algorithm

The programming for simulation was done using Matlab R2016. At the beginning the forward fast Walsh transform / discrete cosine transform is applied to the input image. Then the zonal sampling selection shapes depends on the low- and high-pass filters is performed. The flowchart of the analysed algorithm is shown in Fig. 1.

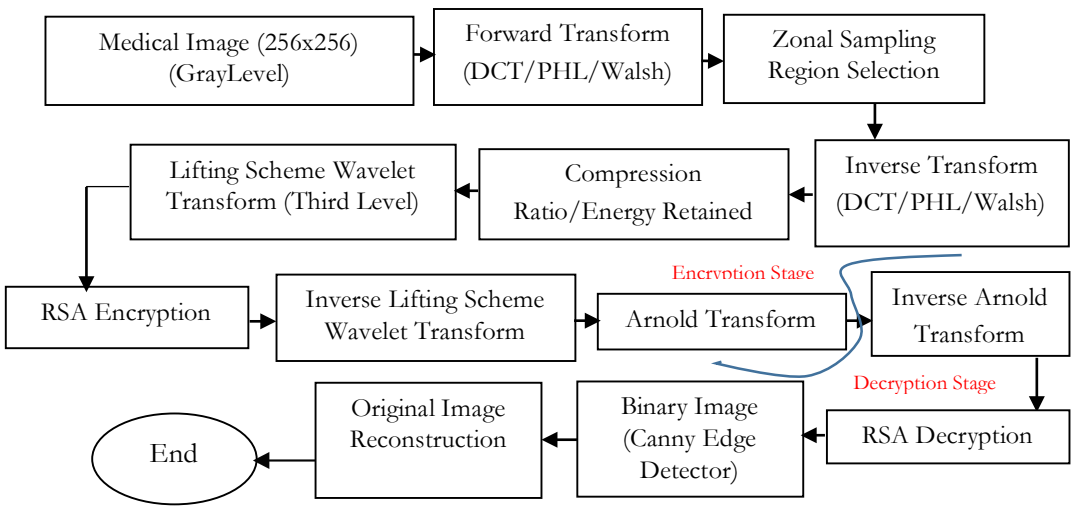


Figure 1: *General scheme for contour extraction from image encryption/decryption*

8 Applied Measures

- Energy: $$E = \sum_{i=1}^{n} \sum_{j=1}^{m} |X(i,j)|^2 \quad (4)$$

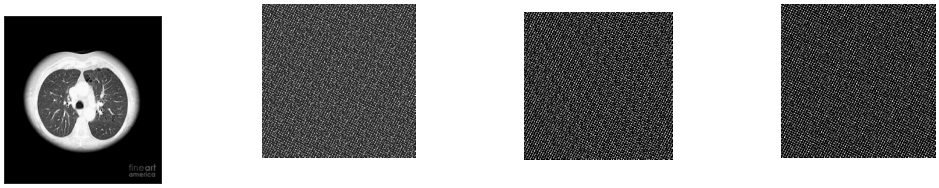
Where *X(i,j)* is the spectral coefficients, and *n* and *m* is the number of rows and columns respectively.

- Compression Ratio: $$CR = \frac{NOZ}{(n*m)} * 100\% \quad (5)$$

Where: *NOZ* is Coefficients number in the desired zonal shape used as LPF filter and $n * m$ is size of the image.

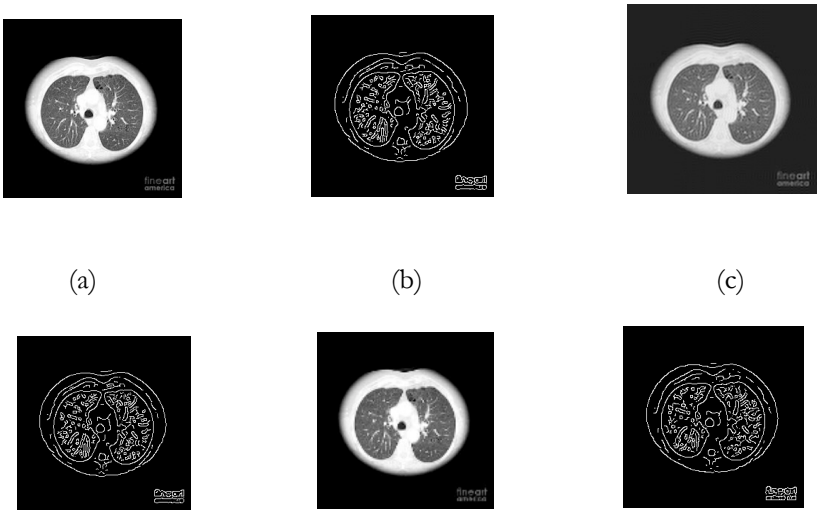
9 Experiments Results

One image is tested by the proposed analyzed algorithm and shown in Fig. 2 (a). Some experiments results for encrypted image using analysed different algorithms are shown in Fig. (b-d). The reconstructed image and contour extraction at the receiver using proposed algorithms are shown in Fig. 3 (related results are in Table I).



(a) (b) (c) (d)

Figure 2: (a) Original image, (b) Encrypted image using Walsh-LWT-RSA-Arnold, (d) Encrypted image using DCT-LWT-RSA-Arnold, and (e) Encrypted image using PHL-LWT-RSA-Arnold



(a) (b) (c)

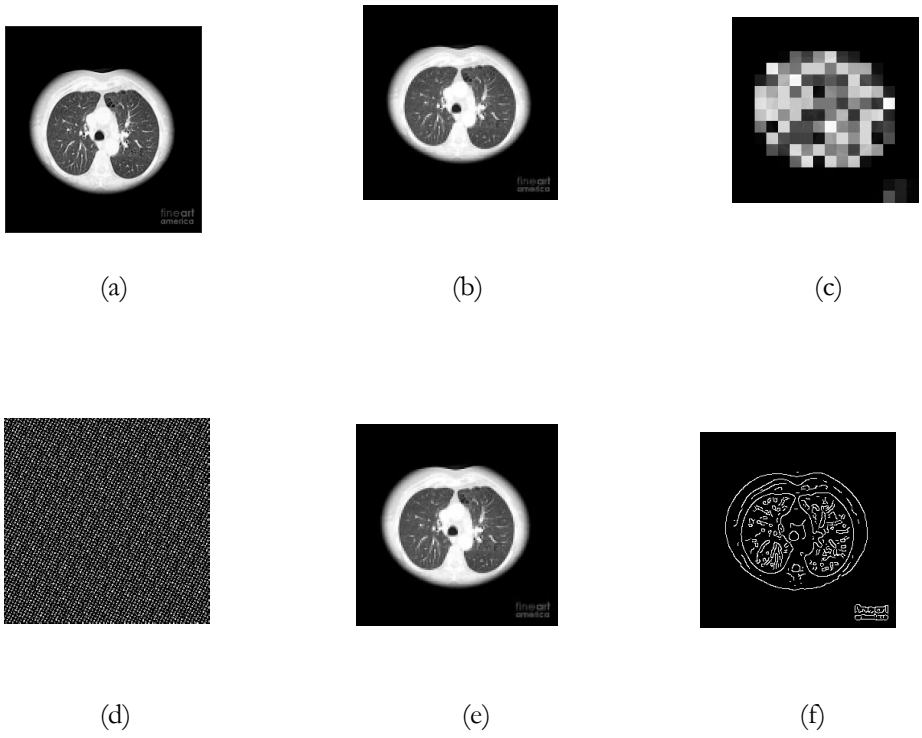
(d) (e) (f)

Figure 3: Image reconstruction and contour extraction from image reconstruction (a, b) Using LWT-RSA-Arnold, (c, d) Using DCT-RSA-Arnold, and (e, f) Using PHL-RSA-Arnold

Table 1: *Summary of formatting requirement for the conference papers*

Method	*Contours Points*	*Retained Energy ER* [%]	*Compression Ratio* [%]	*Consumed Time (s)*
Walsh-LWT-RSA-Arnold	3890	76.4060	75.0061	1.1250
DCT-LWT-RSA-Arnold	4298	83.6425	75.0000	0.4375
PHL-LWT-RSA-Arnold	4041	84.1257	88.5391	0.3750

The steps experiments results for encrypted image using Walsh-LWT-RSA-Arnold are shown in Fig. 4 for Brain image. The steps experiments results for encrypted image using DCT-LWT-RSA-Arnold & Walsh-LWT-RSA-Arnold are shown in Fig. 5 & Fig.6 respectively for Hand image.



(a) (b) (c)

(d) (e) (f)

Figure 4: Using Walsh-LWT-RSA-Arnold: (a) Original image, (b) Image compression (CR=75.0061% and retained energy ER=76.4060% (c) Encrypted Image before Arnold, (d) Encrypted image after Arnold, (f) Image reconstruction at the receiver, and (g) Contour extraction using Canny detector (3890 Pixels)

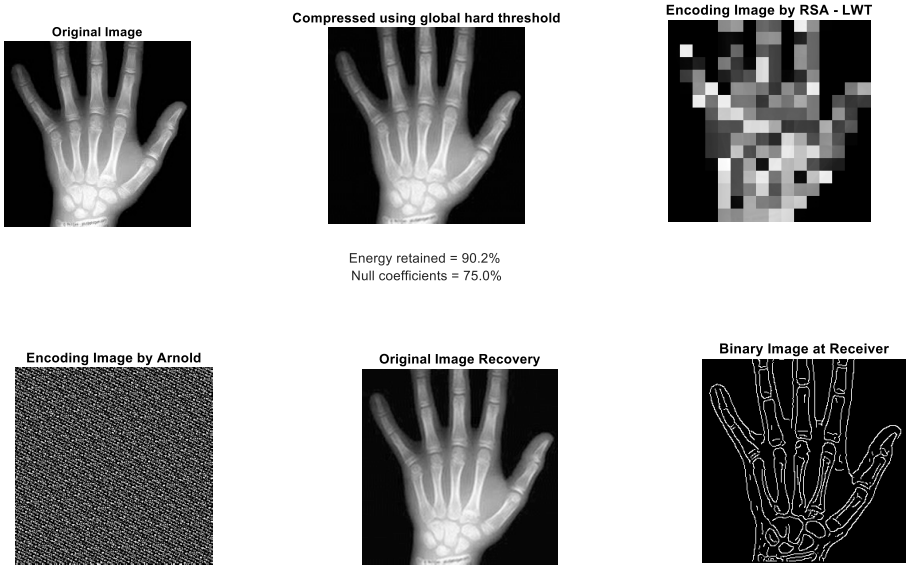


Figure 5: Results of Hand Image using DCT transform (the consumed time is 0.3125 Seconds)

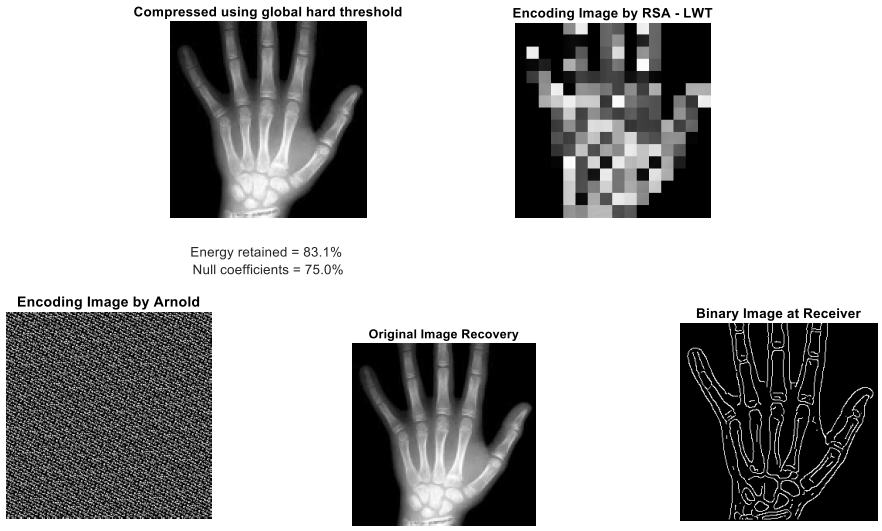


Figure 6: Results of Hand Image using Fast Walsh transform (the consumed time is 3.5320 Seconds)

From the Table I, we were able to know which of the proposed algorithms are the best in accuracy, compression ratio, and quality value of the image in the case of LPF, and we found

that the best one is by using PHL transform; where the value of compression ratio is the higher (88.5391 %); and with higher retained energy (84.1257 %); with lower consumed time.

10 Conclusions

Contour extraction from compressed encrypted medical images by RSA algorithm and Arnold transform can be obtained using this analysed method. Different efficient fast algorithms such Walsh, DCT, and PHL transforms are used for compression purpose. We implemented this technique using Image Processing Toolbox in MATLABR2016. In our experiments, we have investigated the trade-off between consumed time of the reconstructed contour image and number of contour points. Different quality measures were used to assess the quality of the proposed method. The results show that for a compressed medical image at 88.5391%, the total retained energy is saved by 84.1257% using PHL transform if compared with a Walsh and DCT transforms. In addition to that the PHL transform is the fastest one and exceeds to 14.2857% and 66.6667% than DCT and Walsh transforms respectively. However the contour points performed by DCT is the largest compared with other transforms.

References

[1] Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography: Principles and Protocols", ISBN: 978-1-58488-551-1, 2008.

[2] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, "An Introduction to Mathematical Cryptography", ISBN: 978-0-387-77993-5, 2008.

[3] Kalyan Chakraborty, "Introduction to Basic Cryptography", CIMPA School of Number Theory in Cryptography and Its Applications School of Science, Kathmandu University, Dhulikhel, Nepal July 20, 2010.

[4] Vishwagupta, Gajendra Singh ,Ravindra Gupta," Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[5] Sweldens, W. (1995, September). Lifting scheme: a new philosophy in biorthogonal wavelet constructions. In SPIE's 1995 International Symposium on Optical Science, Engineering, and Instrumentation (pp. 68-79). International Society for Optics and Photonics.

[6] Gholipour, M. (2011, June). Design and implementation of lifting based integer wavelet transform for image compression applications. In International Conference on Digital Information and Communication Technology and Its Applications (pp. 161-172). Springer Berlin Heidelberg.

[7] Y. Q. Shi, H. Sun, Image and Video Compression for Multimedia Engineering: Fundamental, Algorithms, and standards, 2nd ed. London: CRC Press Taylor & Francis Group, 2008.

[8] M. Nagabushanam, S. RAMACHANDRAN, and P.KUMAR, "FPGA Implementation of 1D and 2D DWT Architecture using Modified Lifting Scheme, "WSEAS Transactions on Signal Processing, vol. 9, no.4, October 2013, pp. 227-236.

[9] A. Dziech, F. Belgassem & H. J. Nern, Image data compression using zonal zonal sampling and piecewise-linear transforms, Journal of Intelligent And Robotic Systems. Theory & Applications, 28(1-2), Kluwer Academic Publishers, June 2000, 61-68.

[10] S. W. Golomb, G. Gong, Signal Design With Good Correlation: For Wireless Communications, Cryptography and Radar Applications, Cambridge University Press, Cambridge (2005).

[11] L. P. Yaroslavsky, Digital Picture Processing - An Introduction, Springer-Verlag, Berlin (1985).

[12] M. Bossert, E. M. Gabidulin, and P. Lusina, "Space-time codes based on Hadamard matrices proceedings," in Proc. IEEE Int. Symp. Information Theory, Jun. 25–30, 2000, p. 283.

[13] L. Ping, W. K. Leung, and K. Y. Wu, "Low-rate turbo-Hadamard codes," IEEE Trans. Inf. Theory, vol. 49, no. 12, pp. 3213–3224, Dec. 2003.

[14] F. Chabaud, S. Vaudenay, Links between differential and linear cryptanalysis, EUROCRYPT 1994, LNCS vol. 950, pp. 356-365, Springer-Verlag, 1995.

[15] K. Singh and S. Dwivedi, "Digital Watermarking using Asymmetric Key Cryptography and Spatial Domain Technique," International Journal of Advance Research in Computer Science and Management Studies, vol.2, pp. 65-72, August 2014.

[16] A. M. A. Brifcani and W. M. A. Brifcani, "Stego-Based-Crypto Technique for High Security Applications, "International Journal of Computer Theory and Engineering, vol.2, no.6, pp.835-841, December, 2010.

[17] N. Venkatram, L. S. S. Reddy, P. V.V. Kishore, CH. Shavya, "RSA-DWT Based Medical Image Watermarking for Telemedcine Applications," Journal of Theoretical and Applied Information Technology , Vol. 65, No.3, pp.801-812, 31st July 2014.