International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5624-5630

A Secured Model to Reduce the E-Health Record with Lossless BCWT on the Hybrid Cloud

Sudarshan. E[1], Ch. Satyanarayana[2] and C. Shoba Bindu[3]

[1, 3] *Computer Science and Engineering, Jawaharlal Nehru Technological University, Anantapuram, A.P, India.*
[2]*Computer Science and Engineering, Jawaharlal Nehru Technological University, Kakinada, A.P, India.*

[1]*Orcid: 0000-0001-5682-1471*

Abstract

EHR is the patient's health care information system which provides more lucid knowledge about the patient's disease so that the medical treatment can be done in the most appropriate both in terms of manner as well as economy. The patient's HER is upload to the Hybrid Cloud since the basic property of the cloud is its accessibility. The whole health profile of a patient is uploaded and also updated from time to time such as patient's disease, metabolism, MRI, CT scan reports, ECG, Thyroid, etc., So that the corresponding changes in the treatment can be made accurately as per the patient's physiological changes. Over the time such HER's accumulate lots of information which results in the huge database, of which the storage and security problems pop up. The proposed model not only makes the information more secure, but also uses less cloud space by condensing the data. It uses an enhanced Jigsaw puzzle for security and the line based lossless Backward Coding of Wavelet Tree (BCWT) is used to compress the medical images of the EHR and uploaded subsequently to Hybrid Cloud. This BCWT technique saves the internal memory up to 22% and also 15% faster than the existing lossless compression algorithm JPEG2000. This method is 1000 times faster than the AES algorithm. Hence this method is the most appropriate to exploit the fruits of cloud computing technology.

Keywords: EHR, Jigsaw, Hybrid Cloud, AES, BCWT, SPIHT, JPEG2000.

INTRODUCTION

The diverse uses of the information and communication technology have been growing rapidly with the advent of cloud technology because of easy access to the enormous information even remotely in real time. The EHR information can be accessed over the internet and the patients can get the best possible treatment for their ailments from the specialist doctors. The EHR information can be accessed over the internet and the patients can get the best possible treatment for their ailments from the specialist doctors. This will certainly improve the health care globally by putting the information among appropriate professionals.

A. Definitions

"The Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting", defined in [1].

"The resources are needed to render services with the data storage, aggregation, synthesis, retrieval, together with the capacity of computational algorithms and software packages" are called as Cloud Computing[2].

"Where the computing resources conveniently shared a pool of memory on demand that can be plug and play with minimal management effort", defined by NIST [3].

B. Characteristics

The National Institute of Standards and Technology (NIST) also defined five characteristics listed as (i) rapid elasticity (ii) wide range network accessibility (iii) self-services on demand (iv) resource pooling (v) assessed services. The cloud computing system consumes the hardware and software to deliver a service over the internet.

The cloud maintains the information with dynamic resources, high computing power, flexible storage, ubiquitous, convenient, flexible, scalable, available and accessible to a shared pool of configured computing resources (network, software, hardware) from anywhere at any time [8].

C. Services:

Generally speaking, the Fig.1 explains the generic cloud computing architecture with three major layers which cater three following services, namely (i) Platform as a service (PaaS), (ii) Software as a Service (SaaS) and (iii) Infrastructure as a Service (IaaS).

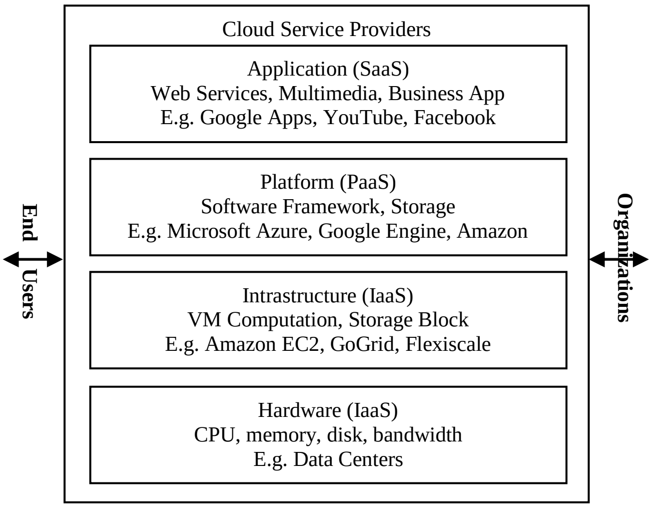

Figure 1: Generic Cloud Computing Architecture

D. Illustrates

The storage of electronic data on floppy, hard discs, CD's, DVD's, micro and macro chips, etc., is on the recording and since the advent of the cloud space. The cloud space providing entrepreneurs such as Dropbox, Amazon, Microsoft Azure, Google Docs, Goole's gmail etc., have effected a paradigm change in the field of virtual data storage, bidding farewell to the physical devices of data storage. This virtual or non material way of data storage can also be of immense use in the field of medicine.

For instance, a cloud based Picture Achieving and Communication system (PACS) [4] is most appropriate to store medical images and can be shared and accessed from all around the globe. Similar to prototype cloud space software designed by Rostrom et al [6], to store and exchange the medical images of radiology [5] between a client and a DICOM server, which is hosted by Microsoft Azure Cloud. There is also 3G and WLAN adaptable Android client by Doukas [7] to access the Amazon cloud.

E. Attentions

Very soon the world is supposed to witness a mushroom growth in the number of cloud space providers because of the following reason. (a) No initial investment, since it is a Pay-as-you-use model. (b) Low operating prices are by dynamic allocation and de-allocation of resources. (c) Easy access is on web based. (d) Low business risks and maintenance free is can be obtained through outsourcing. (e)Highly scalable in rapid resource expansion e.g. Flash-clowd effect or surge computing [9].

F. Opportunities in E-Health

Tremendous developments in the cloud computing technology ushered the following wonderful implications the Health sector. Exchange of patient's E-Health data [10] over the organizations, this reduces the distance between the good doctor and the patient. The patients can be examined by the best doctors available and acquire the best health care possible the research and development activity in the health sector. Since cloud space is a de-regulated field, there is huge scope for designing and developing new standards in maintaining the E-Health cloud data[11,12,13,14].

Hence, it is certain that the EHR data transactions over cloud space will cause a lot of safety and security issues besides storage problems. The EHR information contains radiological images which occupy large space. It would become easier and economic if these images are compressed that they could not consume much space. It is here that the Jigsaw algorithm and Lossless Backward Coding of Wavelet tree (BCWT) [25] come into play, to reduce the image size with zero percentage loss of data, which is also a Hybrid cloud model.

The paper organized as the section 2 discussed with the proposed Hybrid Cloud Architecture. The enhanced Jigsaw puzzle approach is explained in Section 3. The lossless BCWT algorithm compresses the radiological images that discussed in Section 4. The experimental results have been discussed in Section 5. The correlation metrics have discussed in Section 6. The Conclusion and future work explained in Section 7.

THE PROPOSED WORKFLOW OF HYBRID CLOUD ARCHITECTURE

Fig.2 explains the function of Hybrid Cloud Architecture since EHR is a private and personal information it should be saved from cyber trespassing[21]. Hence safety or security or privacy is the major issue addressed here along with compression of the data with zero percentage loss.

a) Every EHR is associated with an ID.
b) The radiological images of patient's information are split into multiple blocks of uniform size.
c) All those uniform boxes are shuffled to form a Jigsaw Puzzle Pattern.
d) Then each block is associated with a random noise with varying colour magnitude.
e) Ultimately with series of permutations the blocks are made undesirable before uploading it to the public cloud.
f) All the about process is stored in a private cloud and re-employed to recreate the original image whenever needed.

The key information which is required to access the data is stored securely in the Private Cloud and the rest of the information stored in Public Cloud. Unauthenticated attempts to access the data can be easily foiled on the Hybrid Cloud.

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5624-5630
© Research India Publications. http://www.ripublication.com

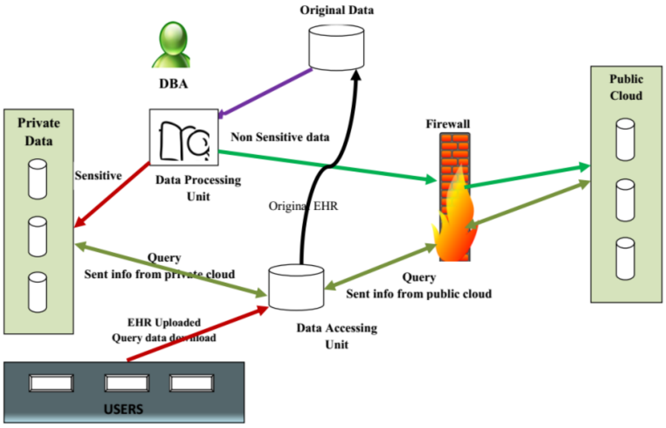

Figure 2: Hybrid Cloud Architecture

The proposed workflow of the method:

Step 1: Read the input image.

Step 2: Apply Jigsaw puzzle approach.

Step 3: Add noise data to resultant image.

Step 4: Lossless BCWT method.

Step 5: Upload the compressed data into the cloud.

Step 6: Apply data scrambling for security.

ENHANCED JIGSAW PUZZLE

Way back in 1964, two scholars namely Freeman and Gardner advocated the Jigsaw puzzle techniques [15]. Later on many variant proposals of jigsaw puzzles came into float with distinct shapes and matching patterns of blocks [16, 17, 18, 19, 20].Jigsaw puzzles have a long history of being the lockers to keep the information secret.

Generally, jigsaw puzzle algorithm is solved in two steps. Firstly, patches are assembled in a fixed pattern, patches are also called as anchor patches as shown in Fig. 3, with a greedy algorithm. Second, divides the original image as multiple equal sizes of blocks and subsequently blocks were shuffled. Here two evidences have considered, dense-and-noisy and sparse-and-accurate used as local evidence for an original image to revert an image.

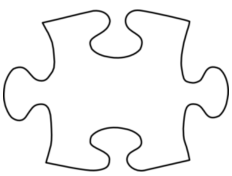

Figure 3: Jigsaw patch

1) Modified Image:

a) Patches addition: Fig.5 shows the addition of patches to an image is for the accuracy as local evidence.

b) Image Division: As shown in Fig.6 the image is divided into *n* number of blocks and each block size could be k x k. Where k is 8, 16, 32, 64,..., 2^n.

Figure 4. Original Image

Figure 5. with Jigsaw patches

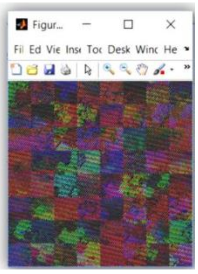

Figure 6. Shuffled image

c) Noise Addition for Each Block: Noise addition for each block. The colour dimension pixel value of every block should substrate with random value between 0 and 255.

2) Image blocks shuffling: Fig.6 shows the outcome of the image after shuffling image blocks.

3) Revert an image: Every attempt of reverting the image by the end user, is informed to both the public and private cloud stake holders.

LOSSLESS BCWT

The Forthcoming generations may completely depend on cloud computing, hence the giant information has grown up. Therefore the compression techniques have leaded the role to make the information concise or compress. The compression techniques lossless JPEG, JPEG-LS and JPEG-XR are not popular due to their limitations. The renowned EZW [22] subsequent algorithm is lossless SPIHT [23].

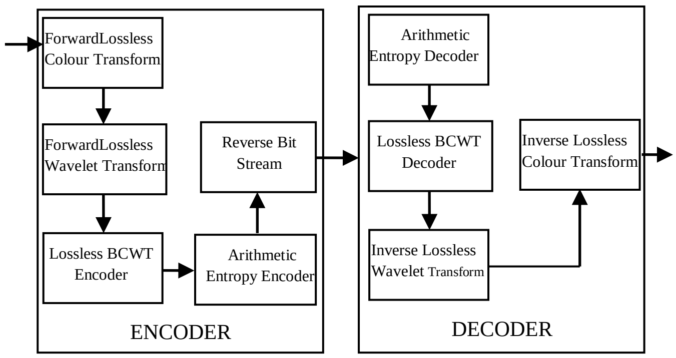

Figure 7: Lossless BCWT Architecture

The SPIHT algorithm was not reached the benchmark, therefore the line-based lossless BCWT algorithm was proposed. Efficiently the lossless BCWT method works on lower end devices fora low cost at high speed computations [24]. The lossless BCWT general architecture is shown in Fig.7 and the Lossless BCWT algorithm execution sequence is depicted in Fig. 8. The lossless BCWT algorithm [24, 25] employs a tree type structure, where the tree nodes are the wavelet coefficients, which generates Maximum Quantization Level (MQL) of descendants of trees and then encoded it when the wavelet coefficient is greater than a threshold, otherwise set wavelet coefficient as ZERO afterwards transmit the bit stream to destination.

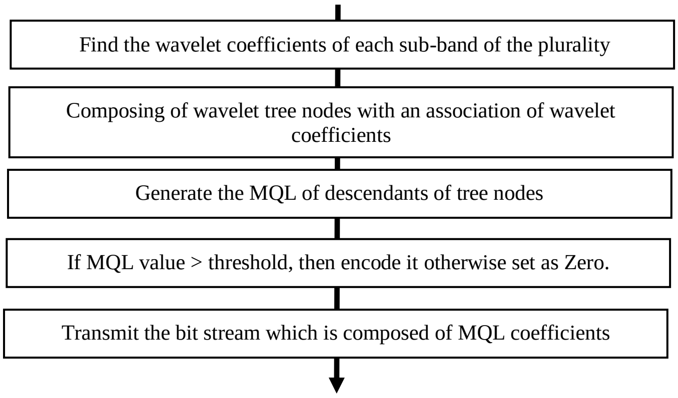

Figure 8: BCWT flow chart

Algorithm for a line of BCWT encoding:

1. Read a line of coefficients as input to BCWT
2. Apply a horizontal 5/3 DWT transformation.
3. Divide the data as low pass and high pass.
4. If a three line buffer filed goto step 6, otherwise goto step 2.
5. Apply a vertical 5/3 DWT Transformation.
6. If it is LL coefficients sent it to the next level of DWT step 10.
7. The coefficients LH, HL and HH shift the buffers and discard the processed data.
8. If coding not formed goto step 2, otherwise goto step 11.
9. If next level DWT is needed goto next-level of the algorithm.
10. BCWT encoding has done and transmits as bits of the stream.

Line-Based Lossless BCWT encoding algorithm:

1. If (*i*,*j*) is in level 3 sub-band, $\forall(k,l) \in O(i,j)$: $m_{k,l} = \max_{(u,v)\in O(k,l)}\{q_{u,v}\}$

2. $q_{L(i,j)} = \max_{(k,l)\in O(i,j)}\{m_{k,l}\}$

3. If $q_{L(i,j)} \geq q_{min}, \forall(k,l) \in O(i,j)$

3.1. If $m_{k,l} \geq q_{min}, \forall(u,v) \in O(k,l)$

3.1.1. If $q_{u,v} \geq q_{min}$, $output\ sign(c_{u,v})$

3.1.2. Output $B(|c_{u,v}|)|_{q_{min}}^{m_{k,l}}$

3.2. Output $T(m_{k,l})|_{\max(m_{k,l},q_{min})}^{q_{L(i,j)}}$

4. $m_{i,j} = \max\left\{\max_{(k,l)\in o(i,j)}\{q_{k,l}\}, q_{L(i,j)}\right\}$

5. If $m_{i,j} \geq q_{min}$, output $T(q_{L(i,j)})|_{\max(q_{L(i,j)},q_{min})}^{m_{i,j}}$

The lossless BCWT algorithm also supports the progressive approach with a region of interest (ROI) and it can rearrange the encoding coding units with their spatial position. The prominent feature is that, the seamless computations will be done in lower end devices also. Hence, the lossless BCWT algorithm is the most appropriate to use in EHR to compress and stores in Hybrid Cloud.

EXPERIMENTAL RESULTS

The Experimental results have done with a PC of I3 processor with a 2.10GHz Intel processor and Windows 2007 operating system with the support of MATLAB 2013b application. The renowned algorithms have deployed to compress HER's image information.

Table I: Comparison of Compression Ratio and Execution Time (MS)

Image Size	Line-Based Lossless BCWT		Line-Based Lossless SPIHT		Line-Based Lossless JPEG2000	
	CR	Run Time	CR	Run Time	CR	Run Time
Artificial (3072x2048)	5.83	0.675	4.18	2.45	6.71	3.68
Building (7216x5412)	2.05	6.763	1.89	35.12	2.17	49.5
Bridge (2749x4049)	1.79	1.971	1.21	7.71	1.9	15.85
Flower (2268x15212)	3.14	0.568	2.32	2.29	3.63	3.47

The lower end devices are conveniently processed for high end compression applications with the support of Line-Based Lossless BCWT algorithm. High-resolution testimonials are used so far in the experiment.

Table II: Comparison of internal memory usage (KB)

Image Size	Line Based Lossless BCWT	Line Based Lossless SPIHT	Line Based Lossless JPEG2000
Artificial (3072x2048)	523.2	5352	2448
Building (7216x5412)	1627.555	33891.890	7597.742432
Bridge (2749x4049)	185.763	7804.1948	866.1891953
Flower (2268x15212)	288.061	24308.398	1342.423718

The result is shown in Table-I, in all testimonials the BCWT compression ratios are almost equal to the JPEG2000, but we observed that a huge difference in an execution time ≈15%. The line-based lossless BCWT algorithm consumes the internal memory is up to ≈22% lesser than the other method and it's shown in Table-II. Therefore, the BCWT algorithm is deployed for compression in a hybrid cloud to process the EHR information.The evaluations have been compared between our proposed algorithm and Advanced Encryption Standard (AES) algorithm with an average time shown in Table-III. The AES algorithm is worked on permutations and substitutions.

Table III: Running time of our algorithm and aes (MS)

Image Size	Image Size After Padding	Proposed Method Time	AES Time	Time Ratio
Artificial (3072x2048)	9437184	76.8717	70617.6	918.6424
Building (7216x5412)	52070656	373.94733	389401.7	1041.328
Bridge (2749x4049)	16394401	119.10180	122390.1	1027.61
Flower (2268x15212)	231404944	1550.8112	1726639	1113.378

The proposed method is more sophisticated than the existing method which developed by AES algorithm and it's all about more than 1000 times faster. Hence the proposed method adoption is most appropriate to exploit faster in the cloud computing technology.

PERFORMANCE METRICS

Once the jigsaw puzzle pieces merged with an image, then the image has to be split into pre-decided size blocks (Dimensions 8x8, 16x16,…. , 2^nx2^n) and make them shuffle. The jigsaw puzzle is NP-Complete problem [28] and latest surveys proposed based on the features of adjacent block's edge of an image can identify the content in polynomial run time. The block wise and pixel wise modification have made more secure shown in Fig. 9.

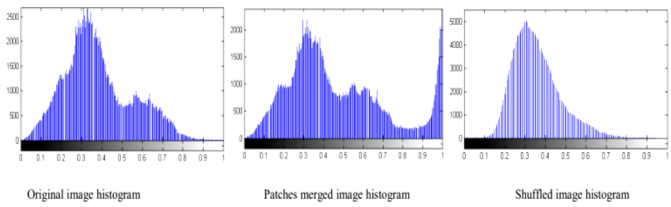

Figure 9: Histograms

$(L_p)^q$ Compatibility:
The compatibility accuracy ratio is about the between of right placement and the number of possible placements as similar of Cho *et al.* [29] and the image jigsaw puzzle was proposed by Cho *et al.*. Let the low-resolution image $X$of blk_i *(right placement block)* associated patch is blk_j *(compatibility placement block)* and i is the local evidence or spatial position index.
The compatibility metric ration should be in the relation, $\forall blk_k \in blocks(X)$

$$C(blk_i, blk_j, R) \geq C(blk_i, blk_k, R). \qquad (eq.1)$$

The dissimilarity compatibility could be measured with different power q of L_p norms. The $(L_p)^q$ color compatibility for the parts of abutting boundaries [29] blk_i , blk_j can be defined as

$$D_{p,q}(blk_i, blk_j, r) = \left(\sum_{k=1}^{K}\sum_{l=1}^{3}\left(\left|\left(blk_i(k,K,l) - rand(i,l)\right) - \left(blk_j(k,1,l) - rand(j,l)\right)\right|\right)^p\right)^{q/p} \qquad (eq.2)$$

The compatibility measure can be defined as

$$C(blk_i, blk_j, R) \propto exp\left(-\frac{D_{p,q}(blk_i, blk_j, R)}{Q(i,R)}\right) \qquad (eq.3)$$

Where *Q(i,R)* is the score of the dissimilarity of all other blocks in R with block blk_i.The dissimilarity accuracy proposed by Cho et al [29], he employed with p=2 and q=2 is substituted in *eq.2*. Hence results are obtained with the power values q=1/16 and p=3/10, therefore,

$$D_{p,q}\left(blk_i, blk_j, r\right) = \left(\sum_{k=1}^{K}\sum_{l=1}^{3}\left(\left|\left(blk_i(k,K,l) - rand(i,l)\right) - \left(blk_j(k,1,l) - rand(j,l)\right)\right|\right)^{\frac{3}{10}}\right)^{\frac{5}{24}} \quad (eq.4)$$

A Taylor's expansion is used to predict the boundaries [30, 31]; a first order prediction would be used for estimating the boundaries of the blocks and it could be verified by employing backward difference estimation using last two neighboring pixels.

In general the $(L_p)^q$ with p=3/10 and 1=1/16 can be expressed by prediction metric P for blk_i, blk_j with relation r;

$$P\left(blk_i, blk_j, r\right) = \sum_{k=1}^{K}\sum_{l=1}^{3}\left[\left(\left[2blk_i(k,K,l) - blk_i(k,K-1,l) - rand(i,l)\right] - blk_j(k,1,l)\right)^{\frac{3}{10}} + \left(\left[2blk_j(k,1,l) - blk_j(k,2,l) - rand(j,l)\right] - blk_i(k,K,l)\right)^{\frac{3}{10}}\right]^{\frac{5}{24}} \quad (eq.5)$$

Here, the image color dimensions block with $K \times K \times 3$ size matrix, $rand(i,l)$ consists an array of random values used to modify the original image.

CONCLUSION

In this paper, we proposed an enhanced data privacy scheme along with the lossless BCWT compression technique. This may have fewer computations with an optimized overhead. The aforementioned design effectively improves the EHR's DICOM image's compression with the help of the line-based lossless BCWT technique. Therefore, this scheme works well even in memory limitation gadgets. The privacy provided gracefully by adding jigsaw puzzle with unique pattern pieces as local evidence in the image along with noise. Afterward, the image divided into blocks and makes them shuffled as randomly. The Line-Based Lossless BCWT is quite well to save internal memory up to ≈22% and the execution time ≈15% has experimentally proven. The proposed method is above the 1,000 times faster than the AES algorithm.

As future work, implement a parallel lossless BCWT algorithm on a parallel platform to grab the tremendous acceleration where the GPGPU (General Purpose Graphics Processing Unit) [26] supports. The CUDA architecture [27] is the most worthy for parallel computing to encourage the parallelism.

REFERENCES

[1] HIMSS, definition EHR, http://www.himss.org/ASP /topics_ehr.asp.

[2] P. Mell and T. Grence, "The NIST definition of cloud computing," Special Publication 800–145 (2011).

[3] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[4] Silva LA et al., "A PACS archive architecture supported on cloud services". Int J Comput Assist Radiol Surg. 2012;7(3):349–58.

[5] Kharat AT et al., "Cloud computing for radiologists". Indian J Radiol Imaging. 2012;22(3):150–4.

[6] Rostrom T and Teng CC. "Secure communications for PACS in a cloud environment." Conf Proc IEEE Eng Med Biol Soc. 2011;2011:8219–22.

[7] Doukas C et al., "Mobile healthcare information management utilizing Cloud Computing and Android OS". Conf Proc IEEE Eng Med Biol Soc.;2010:1037–40.

[8] Q. Zhang, et al., "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7–18, 2010.

[9] Armbrust M et al (2009) "Above the clouds: a Berkeley view of cloud computing. UC Berkeley Technical Report".

[10] AbuKhousa, E.; Najati, H.A. "UAE-IHC: Steps towards Integrated E-Health Environment in UAE." In Proceedings of the 4th e-Health and Environment Conference in the Middle East, Dubai, UAE, 30 January 2012–2 February 2012.

[11] Kaletsch, A.; Sunyaev, A. "Privacy Engineering: Personal Health Records in Cloud Computing Environments." In Proceedings of the International Conference on Information Systems (ICIS 2011), Shanghai, China, 4–7 December 2011.

[12] European Commission. Protecting Your Personal Data. Available online:

http://ec.europa.eu/justice/data-protection/individuals/index_en.htm

[13] U.S. Department of Health & Human Services. Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule.

http://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf

[14] "ITU-T Technology Watch Report—Standards and eHealth,"http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000120003PDFE.pdf

[15] H. Freeman and L. Garder. "A pictorial jigsaw puzzles: the computer solution of a problem in pattern recognition." , IEEE TEC, (13):118–127, 1964.

[16] D. Goldberg et al., “A global approach to automatic solution of jigsaw puzzles.” In Symposium on Computational Geometry, 2002.

[17] W. Kong and B. B. Kimia. “On solving 2D and 3D puzzles using curve matching.” In IEEE CVPR, 2001.

[18] G. Radack and N. Badler. “Jigsaw puzzle matching using a boundary-centered polar encoding.” CGIP, 1982.

[19] H. Wolfson et al.,“Solving jigsaw puzzles by computer.” Annals of Operations Research, 1988.

[20] D. A. Kosiba et al., “An automatic jigsaw puzzle solver.” In IEEE ICPR, volume 1, pages 616–618 vol.1, 1994.

[21] Huang, X., and Du, X. 2013. “Efficiently Secure Data Privacy on Hybrid Cloud.” IEEE International Conference on Communications.

[22] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients,"Signal Processing, IEEE Transactions on, vol. 41, pp. 3445-3462, 1993.

[23] A. Said; W.A. Pearlman, “A new, fast, and efficient image codec based on set partitioning in hierarchical trees,” IEEE Transactions on Circuits and Systems for Video Technology, Vol. 6, June 1996.

[24] Bian Li et.all, “A Line-Based Lossless Backward Coding of Wavelet Trees **(**BCWT) and BCWT Improvements for Application”, dissertation of Texas Tech University, May 2014.

[25] J. Guo, S. Mitra, B. Nutter, and T. Karp, "A fast and low complexity image codecbased on backward coding of wavelet trees," in Data CompressionConference,2006. DCC 2006. Proceedings, 2006, pp. 292-301.

[26] https://en.wikipedia.org/wiki/Graphics_processing_unit.

[27] https://en.wikipedia.org/wiki/CUDA.

[28] E. Demaine and M. Demaine, “Jigsaw puzzles, edge matching, and polyomino packing: Connections and complexity,” Graphs and Combinatorics, vol. 23, 2007.

[29] T. S. Cho, M. Butman, S. Avidan, and W. T. Freeman.“The patch transform and its applications to image editing,” In IEEE CVPR, 2008

[30] Dolev Pomeranzet al.,“A fully automated greedy square jigsaw puzzle solver”, In the Proceedings of the IEEE conference on Computer Vision and Pattern Recognition (CVPR), 2011.

[31] T. S. Cho, S. Avidan, and W. T. Freeman.“A probabilistic image jigsaw puzzle solver.” In Proc. CVPR, pages 183–190, 2010.