JOURNAL OF ENGINEERING RESEARCH & SCIENCES

JENRS

www.jenrs.com
ISSN: 2831-4085

Volume 1 Issue 7
July 2022

EDITORIAL BOARD

Editor-in-Chief

Editorial Board Members

Editorial

In an era dominated by data, where every click and keystroke leave a digital footprint, safeguarding privacy and ensuring security are paramount concerns. The recent surge in technological advancements has ushered in a new age of innovation, offering promising solutions to age-old challenges. This editorial delves into the transformative potential of cutting-edge 7 research papers across various domains, ranging from medical imaging to telemedicine and beyond.

The digitization of medical records and the widespread adoption of imaging technologies have revolutionized healthcare delivery. However, the inherent sensitivity of medical data necessitates robust measures to safeguard patient privacy. The research paper exploring encryption techniques within medical imaging data presents a compelling solution to this pressing issue. By employing sophisticated algorithms based on region of interest (ROI) analysis and histogram peak techniques, the proposed method not only ensures data security but also minimizes the risk of information leakage. Through meticulous evaluation and benchmarking, the study underscores the efficacy of this innovative approach in enhancing data confidentiality without compromising image integrity [1].

In the realm of data anonymization, preserving privacy while retaining data utility poses a formidable challenge. The research paper elucidating a privacy-preserving text document summarization framework offers a beacon of hope in this regard. By categorizing documents based on sensitivity context and leveraging advanced summarization techniques, the proposed system adeptly navigates the delicate balance between anonymity and information retention. With impressive metrics showcasing substantial compression rates and high precision-recall values, this pioneering research paves the way for comprehensive privacy preservation in text analytics, thereby fostering trust in data-driven domains [2].

Amidst evolving societal norms and expectations, understanding the impact of gender on educational experiences remains a pertinent area of inquiry. The study investigating the influence of lecturer gender on learning outcomes among college students sheds light on nuanced preferences and perceptions. Through meticulous data collection and analysis, the research unveils insightful findings regarding student preferences for teaching styles and approaches. By advocating for an inclusive teaching atmosphere that transcends gender biases, the study advocates for fostering collaborative environments conducive to learning and growth [3].

In an increasingly interconnected world, securing digital assets against malicious threats is of paramount importance. The research endeavour delving into image hashing techniques, particularly focusing on SHA-3 algorithms, offers a robust framework for ensuring data integrity and reliability. By harnessing FPGA-based implementations and incorporating optimizations to bolster throughput and efficiency, the study showcases the transformative potential of cryptographic protocols in fortifying data security. With meticulous experimentation and comparative analyses, the research underscores the superiority of SHA-3 in mitigating vulnerabilities and enhancing overall system resilience [4].

The pursuit of technological excellence often hinges on meticulous design and rigorous analysis. The comprehensive review paper elucidating the intricacies of air spring technology underscores the pivotal role of finite element analysis (FEA) in optimizing performance and durability. By delving into the manufacturing process and material considerations, the study offers invaluable insights into enhancing spring stiffness and puncture resistance. Through a judicious blend of theoretical frameworks and experimental validation, the research sets a precedent for advancing engineering solutions in pneumatic systems [5].

The global health crisis precipitated by the COVID-19 pandemic has underscored the imperative for innovative healthcare solutions. The research endeavour elucidating a telemedicine platform for real-time monitoring and analysis of vital parameters heralds a paradigm shift in healthcare delivery. By leveraging wearable sensor networks and advanced data processing techniques, the proposed solution empowers remote patient monitoring while facilitating informed decision-making by healthcare authorities. With a robust infrastructure encompassing software interfaces and wireless sensor connectivity, the research holds immense promise in mitigating the impact of infectious diseases and bolstering public health resilience [6].

In the realm of structural health monitoring, optical fiber sensing technologies offer unparalleled precision and reliability. The research paper delineating the application of optical fiber sensors in fault diagnosis of rotating parts exemplifies the transformative potential of advanced sensing techniques. Through sophisticated signal processing algorithms and quantitative analysis, the study enables accurate extraction of fault characteristics, thereby facilitating proactive maintenance strategies and minimizing downtime. By elucidating the working principles of optical fiber intelligent composite materials, the research underscores the pivotal role of sensor fusion in enhancing predictive maintenance capabilities across diverse industrial domains [7].

In conclusion, the aforementioned research endeavours epitomize the relentless pursuit of innovation in addressing multifaceted challenges spanning privacy preservation, data security, educational dynamics, technological advancements, healthcare delivery, and industrial automation. By harnessing the collective wisdom of interdisciplinary research and embracing cutting-edge methodologies, we can usher in a future defined by resilience, efficiency, and inclusivity. As editors, let us continue to champion excellence and foster a culture of collaboration that transcends boundaries and propels humanity towards a brighter tomorrow.

References:

[1] K. Kiran, S.K. D S, B. K N, H. Rohith, S.K. A J, G.K. M T, “Histogram Based Visible Image Encryption for Real Time Applications,” *Journal of Engineering Research and Sciences*, vol. 1, no. 7, pp. 1–6, 2022, doi:10.55708/js0107001.

[2] A.N.R. Shree, K. P, “Privacy Preserving Text Document Summarization,” *Journal of Engineering Research and Sciences*, vol. 1, no. 7, pp. 7–14, 2022, doi:10.55708/js0107002.

[3] G. Amidu, “Impact of Gender of Lecturers’ on Learning among the College of Arts and Commerce Students’ at Andhra University,” *Journal of Engineering Research and Sciences*, vol. 1, no. 7, pp. 15–19, 2022, doi:10.55708/js0107003.

[4] A. Sideris, T. Sanida, D. Tsiktsiris, M. Dasygenis, “Acceleration of Image Processing with SHA-3 (Keccak) Algorithm using FPGA,” *Journal of Engineering Research and Sciences*, vol. 1, no. 7, pp. 20–28, 2022, doi:10.55708/js0107004.

[5] K.S. Harsh, S. Razdan, “A Review on Materials and Experimental Process used in Air-sprig,” *Journal of Engineering Research and Sciences*, vol. 1, no. 7, pp. 29–37, 2022, doi:10.55708/js0107005.

[6] M. Touil, L. Bahatti, A. El Magri, “Advanced Medical Telemonitoring for the Suspected Cases of Covid-19 Virus,” *Journal of Engineering Research and Sciences*, vol. 1, no. 7, pp. 38–43, 2022, doi:10.55708/js0107006.

[7] M. Zhang, Y. Hua, C. Chen, C. Chu, X. Zhang, “Research on Feature Extraction Method of Fiber Bragg Grating Vibration Monitoring Based on FFT,” *Journal of Engineering Research and Sciences*, vol. 1, no. 7, pp. 44–47, 2022, doi:10.55708/js0107007.

Editor-in-chief

Prof. Paul Andrew

JOURNAL OF ENGINEERING RESEARCH AND SCIENCES

Volume 1 Issue 7 **July 2022**

CONTENTS

Received: 18 February 2022, Revised: 11 June 2022, Accepted: 26 June 2022, Online: 18 July 2022

DOI: https://dx.doi.org/10.55708/js0107001

Histogram Based Visible Image Encryption for Real Time Applications

Kiran * [1], **Sunil Kumar D S** [2], **Bharath K N** [3], **Harshitha Rohith** [4], **Sharath Kumar A J** [1], **Ganesh Kumar M T** [4]

[1] Department of ECE, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
[2] Department of Computer Science, Mangalore University, Mangalore, India
[3] Department of ECE, DSATM, Bangalore, India
[4] Department of ECE, G Madegowda Institute of Technology, Bharathinagara, Mandya Karnataka, India
* Corresponding author: Kiran, Contact No: 8951448999 & Email: kiran.mtech12@gmail.com

ABSTRACT: Like most patient information, medical imaging data is subject to strict data protection and confidentiality requirements. This raises the issue of sending the data which contains a medical image on an open network as per the above issue, also there might be a leakage of information. Encrypting an Image and hiding the information in it is the Potential way of avoiding this problem. But there might be many problems when we try restoring the original image. As a solution to that, an algorithm dealing with region of intrest (ROI) in medical images based on the pixels of interest and histogram peak technique. Firstly Image histogram peak technique is used for calculating peaks in medical images. Then set the Threshold value to segregate the pixels of interest in the medical images. The threshold value can be calculated by taking an average of all peaks in the histogram. These pixels are encrypted with the help of the Sudoku matrix. The proposed scheme will be evaluated using a various test based on statistics along with those results which will be compared to benchmarks of the existing work. We can see the better performance in terms of security from the proposed technique.

KEYWORDS: Region of interest, Medical Images, Encryption, Histogram, Peak Detection

1. Introduction

Medical imaging research has made remarkable progress as a result of increased and improved investment in multimedia technology. The medical image contains the patient's important personal privacy information. Medical images are usually encrypted to protect sensitive content. Common methods used for encrypting are International Data Encryption Algorithm, Data Encryption Standard to protect text data is commonly used [1]. We can see the distribution of pixels is uneven in data of Medical image with good resolution and various features. Regular cryptography used for image protection is not perfect to protect images from digital imaging and communication (DICOM) in medical care because of its inefficiency to handle huge data.

Observing the existing literature, the main issues of telemedicine are as follows. Traditional environments and cryptographic systems are:

- Secure medical images without loss of quality
- Maintain the reliability of confidential medical imaging data.

The aim of the proposed work includes three elements for the rapid and safe transmission of medical images.

- Confidentiality of Medical Images
- Integrity of Areas of Interest of medical images
- Safe recovery of images for diagnosis

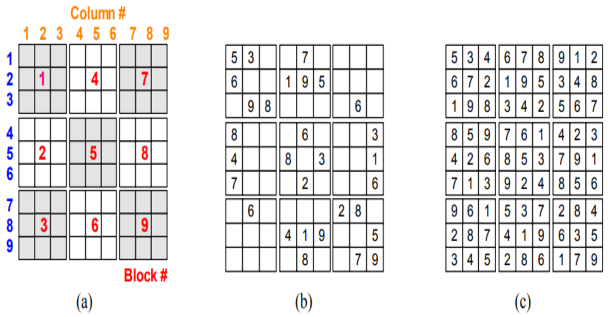
The rest of the sections are as follows. Section 2 explained about various methods related to medical image encryption. Section 3 explains the basic concept of Sudoku used in the proposed encryption method. Section 4 explains the proposed work. Section 5 gives the performance analysis and finally, section 6 gives the conclusion of the work.

2. Related Works

In [2] authors proposed medical imaging is an effective and essential secondary information source they look into when a patient is to be diagnosed by a medical person. The faster way to share medical images is usually through an open network like email or file sharing. These methods will lead to copyright problems, illegal copy, and manipulation of the content. In [3] authors explained into medical image security focused on image encryption and information hiding has grown. In [4] authors explained a simple but efficient method by using matrix multiplication to change the value of a pixel in an image, which made the algorithm very simple but also made it very difficult for intruders to extract the information in the images. In [5] authors described abut 5-D hyperchaotic map actually the result of combining a logistic map with 3D Lorenz, which exhibited dual operating modes. One of the modes focuses only on the pixels obtained from clear text images while the other mode performs diffusion twice in order to obtain secured images. In [6] authors addressed the security issue made the confidential data from the web users be shared on web applications without fear and hence preserving their privacy. In [7] authors explained the improved chaotic map to obtain more security by identifying its drawbacks, followed by the introduction of a modified version of chosen plain text attack. In [8] authors described how to select the most important part of a medical image to hide confidential data. In [9] authors came up with partial encryption of images with secret data in images using FF3-1 and FF1. Without varying the size of the data, encryption of confidential data is done to reduce the usage of storage. In [10] authors introduce the grayscale encryption technique based on ROI with chaos. Using the Edge detection technique (Sobel), extraction of the ROI part is done. Lorenz's system encrypts the sine map and ROI part which are required for the encryption. In [11] authors present a self-generating region of interest (ROI) method for watermarking application in biomedical images. This technique is robust enough to prevent many attacks such as Gaussian, median, sharpening, and wiener filters, which is the major advantage over other methods. In [12] authors discussed a new method to recover the information lossless from encryption in the transform domain. In [13, 14, 15, 16] authors come across a novel lossless game theory-based medical image encryption scheme with optimized ROI parameters along with ROI hidden positions. In [17] authors propose an HS method to examine the hidden lossless data in high-resolution medical images. Use high correlation for the smooth surface of medical imaging anatomy in the local block pixels of the image. In [18, 19] authors described about histogram peak detection of image is a fundamental technique for digital image processing that can be used directly and effectively for image segmentation, quality assessment, enhancement, and data reduction. In [20, 21, 22, 23] authors proposed the conventional indirect method to derive peak values. It consists of two steps. The first step is to fit the data to obtain a P D F. The second step is to calculate the derivative of the PDF to obtain significant peaks.

3. Sudoku Matrix

Here we define a Sudoku matrix as an X * X matrix containing numbers from 1 to N, but since X is the square of the number and N = X, each number occurs only once in each row. Increase only once in each column, only once in each block. Figure 1 below shows an example of a Sudoku puzzle and a solution for X = 9. The solution to the Sudoku puzzle is called the Sudoku matrix [24].



(b)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

(c)

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Figure 1: (a) Showing the Row's no., Column's no. and Block's no.; (b) Example of Sudoku puzzle; (c) Solution for the given puzzle

4. Proposed Visible Encryption Work

Block diagram of proposed selective image encryption system as shown in figure 2. The proposed system includes different steps for selecting and encoding regions of interest in medical images. First, calculate the histogram peak of the original medical image using the peak detection technique and as shown in Figure 3. The peak detection algorithm first generates a peak detection signal from the image histogram. The peaks in the histogram are then determined using the extreme point between the zero and zero intercepts of the peak detection signal. Convolution uses the first derivative approximation discriminator. For an ideal smooth histogram, the peak can be determined from the sign and zero intersection of the signal obtained from the h and S convolutions. The zero intersection estimates the extreme points of the histogram and the position of the turning point. The `*` symbol in figure 3 indicates the maximum values of the original medical image. The threshold value for separating the important pixels of the medical image can be calculated by taking the average of all the peak values obtained when the histogram peak is detected. Then compare each pixel of the original medical image with the threshold value, and if it is above the threshold value, group them into meaningful blocks of pixels. Sudoku matrix of multiples of 16*16 randomly generated for diffusion operation. Using pixels in a sudoku matrix, randomly encrypt a block of important pixels by performing an XOR operation.

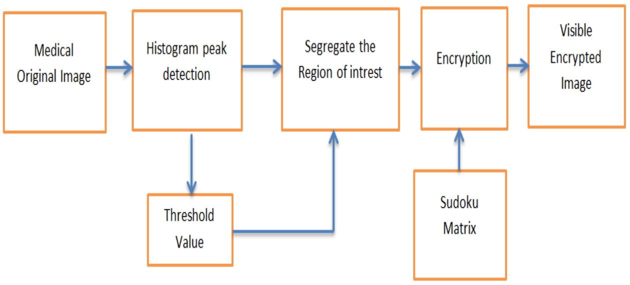


Figure 2: Proposed technique's Architecture

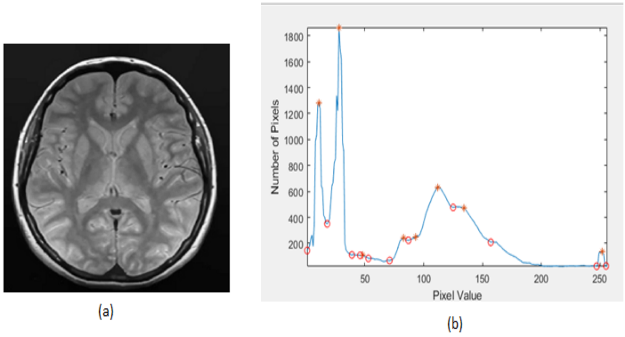


Figure 3: (a) Original MRI image (b) Peak detection using Histogram

Algorithm for encryption process:

- **Step 1:** Load the original medical image of size p*q.
- **Step 2:** Determine the histogram of original medical image.
- **Step 3:** Apply the histogram peak detection technique to extract all the possible peaks in the input image histogram.
- **Step 4:** Calculate the threshold value by averaging all the obtained peaks values.
- **Step 5:** Compare the every pixels in the original medical image with threshold value. If it is greater, then store the pixel into significant block.
- **Step 6:** Construct the Sudoku matrix with a same size of significant block.
- **Step 7:** Finally visible encrypted image is produced by performing XOR operation between significant block pixels and random pixels in the sudoku matrix.

5. Results and Discussion

The proposed technique is analyzed by evaluating the various parameters. Below are the parameters involved in this.

5.1. Analysis of Entropy

The amount of randomness is evaluated by Entropy in a cryptographic system. Equation of Entropy is [25-26]:

$$H(S) = \sum_{i=0}^{2^M-1} P(si)\, log_2 \frac{1}{P(si)} \qquad (1)$$

where P (si) gives the probability of ith gray-level occurring in the image. Ideal entropy value for a random image is 8. If it is low, it is more predictable. Table 2 gives sample image's entropy along with its respective cryptographic image.

5.2. M S E (Mean Square Error)

M S E is generally analyzed by averaging the squares of the difference between scrambled and plain scrambled image. Higher the value of M S E, the higher the encryption and the more noisy the clear image. The formula for MSE [27] given by.

$$MSE = \frac{1}{MXN}\sum_{i=1}^{M}\sum_{j=1}^{N}[inp(i,j) - enc(i,j)]^2 \qquad (2)$$

5.3. P S N R(Peak Signal to Noise Ratio)

PSNR is always the reciprocal of the mean squared error (M S E). Increase MSE and reduce PSNR for better image security. Mathematically, the PSNR is given as follows [28].

$$PSNR = 10\, log_{10}\frac{255}{MSE} \qquad (3)$$

5.4. UACI and NPCR

NPCR stands for number of pixel change rate and UACI is unified avarage change intensity defins as follows [29].

$$UACI = \frac{1}{N}\left[\sum_{i,j}\frac{|C1(i,j)-C2(i,j)|}{255}\right] \qquad (4)$$

$$NPCR = \frac{\sum_{i,j}D(i,j)}{MXN}X100\% \qquad (5)$$

here n and m gives the number of columns and rows respectively. D(i, j) is given by

$$D(i,\ j) = \begin{cases} 1, C1(i,j) \neq C2(i,j) \\ 0, \qquad otherwise \end{cases} \qquad (6)$$

here cipher and original images are given by C2(i, j) and C1(i, j) respectively.

5.5. U I Q(Universal Image Quality Index)

To extract the similarity between cipher and original image we use U I Q. It is ranging from -1 to +1 where the more similarity is indicated by the 1 and least similarity is indicated by -1. Equation for U I Q is [29].

$$UQI(x,y) = \frac{\sigma xy}{\sigma x\sigma y} * \frac{2\mu x\mu y}{\mu x^2+\mu y^2} * \frac{2\sigma x\sigma y}{\sigma x^2+\sigma y^2} \qquad (7)$$

5.6. S S I M(Structural Similarity Index Measure)

U I Q Index's improved version is S S I M. It is ranging from -1 to +1 where the more similarity is indicated by the 1 and least similarity is indicated by -1. Equation for S S I M is [29].

$$SSIM(x,y) = \left[\frac{(2\mu x\mu y+C1) \quad (2\sigma xy+C2)}{(\mu x^2+\mu y^2+C1) \quad (\sigma x^2+\sigma y^2+C2)}\right] \qquad (8)$$

here, when the division is done with weak denominator, to stabilize that we use the constants C2 and C1.

Table 1: Results of proposed work

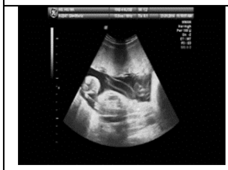
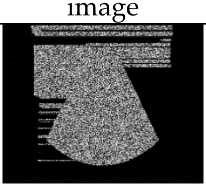
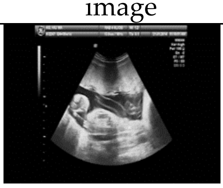
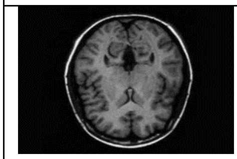
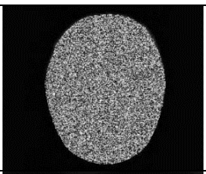
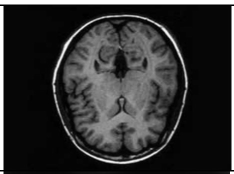
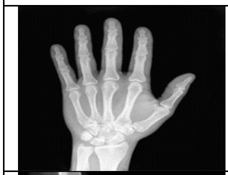
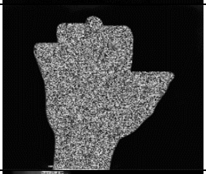
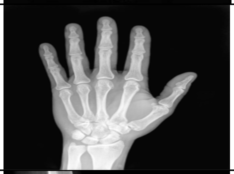
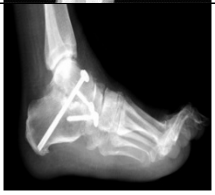
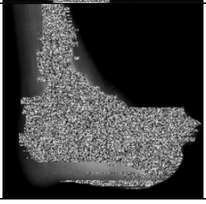
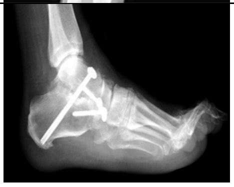
Medical Image	Encrypted RoI image	Decrypted RoI image
		
		
		
		

Table 2: ROI based encryption system's parameters Performance

Image	Entropy Input	Entropy output	MSE	PSNR (db)	NPCR (%)	UACI (%)	UQI	SSIM
Hand	4.4402	6.0012	76.62	59.89	49.07	25.10	0.74	0.42
MRI	4.5598	5.9972	53.70	42.85	44.02	19.69	0.68	0.47
Foot	3.7643	5.0887	89.12	72.20	46.95	30.62	0.81	0.54
Baby	4.9216	6.4233	46.13	23.95	47.89	26.68	0.60	0.46

Table 3: ROI based encryption system's Efficiency

Name of Image	Time elapsed for Encryption (sec)	Percentage of Time saved
Hand	0.15953	46.6564
MRI	0.17435	45.6093
Foot	0.198069	39.5001
Baby	0.171694	44.7968

Table 1 shows the inputs images, encrypted images and decrypted images of proposed system. From Table 2, we conclude that the entropy value of the encoded image is greater than the entropy value of the original simple image. The MSE score is increased based on the image showing the level of encoding. With selective encoding, the NPCR values of the proposed method do not change significantly, the cost and computation time are reduced, and the same metrics are reduced to zero. In other words, the lower the value, the higher the difference between them. Input image and encoded ROI image.

Table 3 shows the effectiveness of the proposed method in terms of speed of implementation and cost. Compared with full-frame encoding, this method saves about 50% of computation cost and provides fast frame-coding execution time. The analysis of the entropy values of the various medical images in Table 2 reveals the high entropy of the new cryptographic algorithms.

Table 2 calculated the SSIM values between the final encoded medical image and the original medical image. Obviously, our method gives a smaller SSIM value. From Table 3, we can see that the coding time for different medical images has been reduced. This is achieved because it performs image selective encoding rather than full encoding, and because it is a lightweight encoding technology, it takes less time to perform bit-plane encoding.

Table 4: Comparison of MRI Image's Parameter with other method

Parameter	Proposed Technique	Method [30]	Method [31]
MSE	53.7086	86.2657	123.56
PSNR (db)	42.8534	10.0881	25.45
NPCR (%)	44.0204	51.47	65.78
UACI(%)	19.6987	12.4578	18.91
SSIM	0.4718	0.4621	0.65
Encryption Time(secs)	0.17435	72.5001	32.25

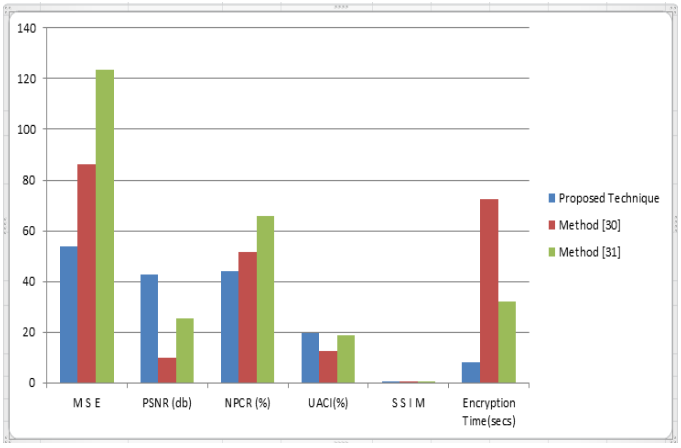


Figure 8: Comparison of performance parameters with existing methods [30, 31]

Our method significantly reduces encryption time, ensures the reliability of images sent to the cloud, and ensures security with a two-level encryption scheme. To check the validity of the selective encoding scheme, calculate various parameters such as NPCR, MSE, PSNR, SSIM, and encoding time and compare these values with those obtained by existing methods. Table 4 shows that selective encryption schemes are an effective method because they give better results than existing methods.

6. Conclusion

In this article, we have proposed a method to partially encrypt personal information such as tumors and fetal organs. Traditional image protection technologies have many problems such as data filling up and growing larger as storage space is wasted over time. Furthermore, since the entire image is encrypted, the image cannot be recognized before decryption and sensitive information is leaked after decryption. The problem of conventional sub-image encryption is that the unnecessary parts are encrypted by encrypting a rectangular region consisting of pieces of information requiring security. The proposed method detects important pixels using histogram vertex detection and counts them using Sudoku matrix. In this study, we measure the encryption speed of the proposed method and determine the most suitable block unit for encryption in order to improve the encoding and decoding speed of the image part. Limitation of proposed work is not applicable to binary image encryption.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] H. Satoh, N. Niki, K. Eguchi, H. Ohmatsu, M. Kusumoto, M. Kaneko, and N. Moriyama, "Teleradiology network system on cloud using the web medical image conference system with a new information security solution," in Medical Imaging 2013: Advanced PACS-based Imaging Informatics and Therapeutic Applications, vol. 8674, pp. 264-272, SPIE, 2013. DOI: 10.1117/12.20069831.

[2] T. Avudaiappan, R. Balasubramanian, S. Sundara Pandiyan, M. Saravanan, S. K. Lakshmanaprabu, and K. Shankar, "Medical image security using dual encryption with oppositional based optimization algorithm," Journal of Medical Systems, vol. 42, no. 11, pp. 1-11, 2018. DOI: 10.1007/s10916-018-1053-z2.

[3] C. Wang, X. Wang, Z. Xia, and C. Zhang, "Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm," Information Sciences, vol. 470, pp. 109-120, 2019. DOI: 10.1016/j.ins.2018.08.0283.

[4] D. Xie, "Public key image encryption based on compressed sensing," IEEE Access, vol. 7, pp. 131672-131680, 2019. DOI: 10.1109/ACCESS.2019.29409964.

[5] S. Zhu and C. Zhu, "Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map," IEEE Access, vol. 7, pp. 147106-147118, 2019. DOI: 10.1109/ACCESS.2019.29462085.

[6] M. Binjubeir, A. A. Ahmed, M. A. B. Ismail, A. S. Sadiq, and M. K. Khan, "Comprehensive survey on big data privacy protection," IEEE Access, vol. 8, pp. 20067-20079, 2019. DOI: 10.1109/ACCESS.2019.29623686.

[7] M. Li, P. Wang, Y. Liu, and H. Fan, "Cryptanalysis of a novel bit-level color image encryption using improved 1D chaotic map," IEEE Access, vol. 7, pp. 145798-145806, 2019. DOI: 10.1109/ACCESS.2019.29409964.

[8] G. Manjula and H. S. Mohan, "Probability based selective encryption scheme for fast encryption of medical images," in ICAICR'19: Proceedings of the Third International Conference on Advanced Informatics for Computing Research, Article, vol. 17, pp. 15-16, 2019.

[9] W. Jang and S.-Y. Lee, "Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment," International Journal of Distributed Sensor Networks, vol. 16, no. 3, 2020. DOI: 10.1177/15501477209147791.

[10] V. Sankaradass, P. Murali, and M. Tholkapiyan, "Region of Interest (ROI) based image encryption with sine map and lorenz system," in International Conference on ISMAC in Computational Vision and Bio-Engineering, Springer, Cham, 2018.

[11] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "A heuristic automatic and robust ROI detection method for medical image warermarking," Journal of digital imaging, vol. 28, no. 4, 2015. DOI: 10.1007/s10278-015-9770-z2.

[12] J. Zhou, J. Li, and X. Di, "A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position," IEEE Access, vol. 8, 2020. DOI: 10.1109/ACCESS.2020.30075503.

[13] P. Rashmi and M. C. Supriya, "Encryption of Color image to enhance security using Permutation and Diffusion Techniques," International Journal of Advanced Science and Technology, vol. 28, no. 12, 2019.

[14] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on circuits and systems for video technology, vol. 16, no. 3, 2006. DOI: 10.1109/TCSVT.2006.8699644.

[15] C. V. Kumar, V. Natarajan, and D. Bhogadi, "High capacity reversible data hiding based on histogram shifting for medical images," in 2013 international conference on communication and signal processing, IEEE, 2013.

[16] Y. Yang, W. Zhang, and N. Yu, "Improving visual quality of reversible data hiding in medical image with texture area contrast enhancement," in 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 81-84, IEEE, 2015. DOI: 10.1109/IIH-MSP.2015.701.

[17] M.-H. Wu, J. Zhao, B. Chen, Y. Zhang, Y. Yu, and J. Cheng, "Reversible data hiding based on medical image systems by means of histogram strategy," in 2018 3rd International Conference on Information Systems Engineering (ICISE), pp. 6-9, IEEE, 2018.

[18] L.-C. Huang, L.-Y. Tseng, and M.-S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images," Journal of Systems and Software, vol. 86, no. 3, pp. 716-727, 2013. DOI: 10.1016/j.jss.2012.11.0242.

[19] X. D. Yue, D. Q. Miao, N. Zhang, L. B. Cao, and Q. Wu, "Multiscale roughness measure for color image segmentation," Information Sciences, vol. 216, pp. 93-112, 2012. DOI: 10.1016/j.ins.2012.05.014.

[20] S. S. Sastry, K. Mallika, B. G. S. Rao, H. S. Tiong, and S. Lakshminarayana, "Liquid crystal textural analysis based on histogram homogeneity and peak detection algorithm," Liquid Crystals, vol. 39, no. 4, pp. 415-418, 2012. DOI: 10.1080/02678292.2011.652198.

[21] S. Boukharouba, J. M. Rebordão, and P. L. Wendel, "An amplitude segmentation method based on the distribution function of an image," Computer Vision, Graphics, and Image Processing, vol. 29, no. 1, pp. 47-59, 1985.

[22] T. Elguebaly and N. Bouguila, "Bayesian learning of finite generalized Gaussian mixture models on images," Signal Processing, vol. 91, no. 4, pp. 801-820, 2011. DOI: 10.1016/j.sigpro.2010.08.0123.

[23] M. Azam and N. Bouguila, "Unsupervised keyword spotting using bounded generalized Gaussian mixture model with ICA," in 2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP), pp. 1150-1154, IEEE, 2015. DOI: 10.1109/GlobalSIP.2015.7418378.

[24] Y. Wu, Y. Zhou, J. P. Noonan, K. Panetta, and S. Agaian, "Image encryption using the sudoku matrix," in Mobile Multimedia/Image Processing, Security, and Applications 2010, vol. 7708, pp. 222-233, SPIE, 2010. DOI: 10.1117/12.853197.

[25] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," computing, vol. 23, 2010.

[26] X. Zhang, L. Wang, G. Cui, and Y. Niu, "Entropy-based block scrambling image encryption using DES structure and chaotic systems," International Journal of Optics, 2019. DOI: 10.1155/2019/35945341.

[27] Y. Wu, J. P. Noonan, and S. Agaian, “NPCR and UACI randomness tests for image encryption,” Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), vol. 1, no. 2, pp. 31-38, 2011.

[28] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: from error visibility to structural similarity,” IEEE transactions on image processing, vol. 13, no. 4, pp. 600-612, 2004. DOI: 10.1109/TIP.2003.8198612.

[29] Z. Wang and A. C. Bovik, “Modern image quality assessment,” Synthesis Lectures on Image, Video, and Multimedia Processing, vol. 2, no. 1, pp. 1-156, 2006. DOI: 10.1007/978-3-031-02238-83.

[30] M. Sajjad, K. Muhammad, S. W. Baik, S. Rho, Z. Jan, S.-S. Yeo, and I. Mehmood, “Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices,” Multimedia Tools and Applications, vol. 76, no. 3, pp. 3519-3536, 2017. DOI: 10.1007/s11042-016-3811-64.

[31] P. T. Akkasaligar and S. Biradar, “Selective medical image encryption using DNA cryptography,” Information Security Journal: A Global Perspective, vol. 29, no. 2, pp. 91-101, 2020. DOI: 10.1080/19393555.2020.17182485.

KIRAN currently working as an assistant professor in department of Electronics and Communication engineering at Vidyavardhaka college of Engineering, Mysuru, Karnataka, India. Kiran received his M.Tech in Digital Electronics and Communication Systems at Malnad College of Engineering - Hassan affiliated to Visvesvaraya Technological University, Belgaum, Karnataka, India. He is currently pursuing his Ph.D at Visvesvaraya Technological University, Belgaum, Karnataka, India. His research interests are related to Human Computer Interaction and medical Image security. He has published several research papers at national and international journals, conference proceedings.

Dr. SUNIL KUMAR D S obtained his ph.d. in computer science from mangalore university, india. he was received his m.sc. in computer science from kuvempu university, india before obtaining his phd. his research area of interest is pattern recognition, machine learning and deep learning. he has published 4 research papers in highly reputed international journals and conference proceedings. his ph.d. research work is on signature biometric. he was worked as faculty member in various institution in bangalore, india. his one of the research paper is published in the isprs international workshop “photogrametric and computer vision techniques for video surveillance, biometrics and biomedicine” -psbb17 held in lomonosov moscow state university, moscow, russia from 15th to 17th of may-2017. the international workshop is organized by isprs wg ii/5 and wg ii/10, the state research institute of aviation system (gosniias, russia), lomonosov moscow state university and the moscow state university of geodesy and cartography (miigaik, russia).

Bharath K N currently working as an assistant professor in department of Electronics and Communication engineering at DSATM, Bangalore, Karnataka, India. Bharath K N received his M.Tech in Digital Electronics and Communication Systems at Malnad College of Engineering - Hassan affiliated to Visvesvaraya Technological University, Belgaum, Karnataka, India. He is currently pursuing his Ph.D at Bangalore university, Bangalore, Karnataka, India. His research interests are related to image compression and medical Image security. He has published several research papers at national and international journals, conference proceedings.

Harshitha R completed B.E. (Electronics and Communication) in 2014 and M.Tech (Signal Processing) in 2016 under V.T.U., Belagavi. She is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering at G Madegowda Institute Of Technology, Bharathinagara, Mandya Karnataka, India. She has over 6 years of teaching experience and has published about 12 papers in various national and international journals and conferences. Her areas of interest include, Communication Systems, Robotics, Image Processing, Signal Processing and Digital electronics. She has also guided a few undergraduate students for their final year project work and also for the funded project under Karnataka State Council For Science and Technology (KSCST).

Dr. Sharath Kumar A J completed his B.E. (Electronics and Communication) in 2010 and M.Tech (Electronics) in 2012 and Ph.D (Antenna Design) in 2021 under V.T.U., Belagavi. He is currently working as a Associate Professor in the Department of Electronics and Communication Engineering at Vidyavardhaka College of Engineering, Mysuru, Karnataka, India. He has over 9 years of teaching experience and has published about 25 papers in various national and international journals and conferences. He is a senior Member IEEE and life member of I.S.T.E. His areas of interest include Microwaves and Antennas, Communication Systems, Robotics, Control Systems and Digital electronics. He has also guided a few undergraduate students for their final year project work.

Dr. Ganesh Kumar M T completed his B.E. (Electronics) in 1984 and M.E(Electronics) in 1992 and Ph.D (GNR FET based 8-bit multiplication design) under Raffles university, Rajasthan. He is currently working as a Professor in the Department of Electronics and Communication Engineering at G Madegowda Institute Of Technology, Bharathinagara, Mandya, Karnataka, India. He has over 35 years of teaching experience and has published about 20 papers in various national and international journals and conferences. His areas of interest include VLSI, image processing and Digital electronics. He has also guided a few undergraduate students for their final year project work.

Received: 17 February 2022, Revised: 11 May 2022, Accepted: 23 June 2022, Online: 18 July 2022

DOI: https://dx.doi.org/10.55708/js0107002

Privacy Preserving Text Document Summarization

A N Ramya Shree *, **Kiran P**

CSE Department, RNS Institute of Technology, Bengaluru,560098, India

* Corresponding author: A N Ramya Shree, Asst.Professor, CSE Department, RNSIT,8971896318 & ramyashree.a.n@rnsit.ac.in

ABSTRACT: Data Anonymization provides privacy preservation of the data such that input data containing sensitive information is converted into anonymized data. Hence, nobody can identify the information either directly or indirectly. During the analysis of each text document, the unique attributes reveal the identity of an entity and its private data. The proposed system preserves the sensitive data related to an entity available in text documents by anonymizing the sensitive documents either entirely or partially based on the sensitivity context which is very specific to a domain. The documents are categorized based on sensitivity context as sensitive and not-sensitive documents and further, these documents are subjected to Summarization. The proposed Privacy Preserving Text Document Summarization generates crisp privacy preserved summary of the input text document which consists of the most relevant domain-specific information related to the text document without defying an entity privacy constraints with the compression rate of 11%, the precision of 86.32%, and the recall of 84.28%.

KEYWORDS: PHI, PPDP, Generalization, and Sanitization

1. Introduction

Nowadays, the vast volume of electronic data is increasingly growing. It may be structured data such as databases, leggy data of the organization, or unstructured data such as text contents, images, videos, etc. Approximately 85 to 90 percent of the information is available in unstructured form as per the Forbes Survey. Related to this healthcare providers, state and private enterprises are progressively storing vast numbers and types of medical data in both online and offline modes. In recent years developments in healthcare have resulted in requirements like the tremendous number of personal health data to be collected, exchanged, and analyzed by organizations. There has been an increase in health data being produced and processed by health agencies as a result of the increasing adoption of the Electronic Health Records (EHR), profoundly stimulated by the Health Information Technology for Economic and Clinical Health Act (HITECH Act 2009). Although secondary use of Clinical data has greatly improved the consistency and reliability of medical science and healthcare administration, due to the common nature of exchanging health records which results in increasing queries regarding patient privacy. The Health Insurance Portability and Transparency Act (HIPAA) has developed a series of privacy guidelines to address these queries in HITECH Act 2009. The HIPAA Safe Harbor law defines altogether 18 types of features that are specifically called as confidential features [1].

Personal Health Information (PHI), which must be deleted before a third party is released with the health data which leads to a lot of research in Privacy Preserving Data Publishing on structured data means data which has a pre-defined format, where numerous techniques have been proposed and developed. Privacy protection approaches for sharing medical documents, focus on the detection and removal of PHI items from the documents using different PPDP (Privacy Preserving data Publishing) approaches like Data Swapping, Data Randomization, Cryptography, and Data Anonymization. Among these Data Anonymization is the popularly used Privacy Preserving Data Publishing approach. Data Anonymization is achieved by Pattern Matching based approaches and Machine Learning based approaches which mainly focused on structured data. In this paper, a Machine Learning-based approach called Privacy Preserving Text Document Summarization has been proposed to preserve the privacy of unstructured data which uses i2b2 discharge summary documents, which are collections of progression of the release report of patients by the Harvard University. The discharge summary documents contain the subtleties of a specific patient These informational collections are old certifiable data and are of type text documents [2].

2. Related Work

Whenever a transcript or confidential report is made about an entity it must be protected to preserve the privacy of an entity or an individual before publishing to the outside world. In general, the real-world data associated with an individual or the entity mainly belongs to a specific domain, related to this the data anonymization approach is also mainly dependent on domain-specific attribute types associated with an individual or the entity [3]. There are four major types of domain-specific attributes that are used in anonymization. 1. Personally Identifiable Information (PII) - Attributes that are directly used to identify an individual who belongs to a specific domain. 2. Sensitive Attributes / Private Attributes (SA / PA) - Attributes that are very specific to an individual, which are not to be disclosed.3.Quasi Attributes (QA) - Attributes that are indirectly used to identify or recognize an individual belonging to a certain domain.4. Not-sensitive Attributes (NSA) - Attributes that are considered common for all individuals belonging to a certain domain.

The PII is removed before when an individual or entity data is subjected to summarization because it discloses an individual identity. The Quasi Attributes are those which are used by the attacker or a malicious third-party data analyst to identify the individual or entity when it is linked with other publicly available data like voter lists, census data, etc. The major types of data transformation approaches used in anonymization are Generalization and Suppression. The data usage domain plays a vital role in anonymization because either data generalization or suppressed operations depend on a specific domain. In generalization, the individual quasi attributes are generalized based on the usage domain such that they should not reveal the actual value. Example: Date of Birth attribute value generalized to Born in Year such that the birthdate is not disclosed. In Suppression, the sensitive and or quasi attributes are replaced by special symbols or removed before their usage in data publishing operation. Table 1 describes different anonymization approaches [4].

In the healthcare domain, the most challenging aspect is preserving the privacy of patients who undergo various disease treatment processes. The major research related to privacy preserving data publishing focuses on structured data. which also depends on the usage domain. The major works include survey about the De-identification of Sensitive information in a patient note with recurrent neural networks in a detail and how it further reveals an individual identity[5]. Document Sanitization, which is a privacy policy that aims to identify critical attributes like name, dob, etc. which further can be either removed or replaced before it is made public. The government has set specific guidelines for maintaining confidentiality. According to medical data, the Health Insurance and Portability and Accountability Act (HIPAA) prescribes all personal identification information in medical records must be removed before it can be made available to the public [6]. The center thought of the k-anonymization model is that each record in a table is unclear from in any event from other k-1 records regarding the pre-decided quasi identifier where a table is used which excludes all explicit identifiers. The secure data is fetched by publishing information with different tricky credits which turns out to be almost certain than some other distribution styles [7] . The k-anonymization model which has been widely contemplated and upgraded as a feasible meaning of protection in information distribution. The decision about the k-Anonymization model depends on various strategies like Speculation, Concealment, and other hybrid approaches. It changes private information over to public information such that it can be used at different levels of data handling [8]. The patient outline details which is a fundamental need for clinicians to give facilitated care and practice powerful correspondence. The computerized outline can save time, normalize notes, help dynamically, and lessen clinical mistakes. They specify an upper bound on the extractive outline of release notes and build up an LSTM model to successively name the history of present sickness notes [9].

Table 1: Anonymization Approaches

Techniques	Parameters	Applications	Limitations
k-anonymity Sweeny et. al.	Sensitive features	Correlation between the rows	only on structured data
l-diversity Ashwin M et. al.	Quasi & Sensitive attributes	Equivalent sensitive attributes groups	common frequency value for a sensitive attribute
t-closeness Ninghui Li et. al.	PII, Quasi, Sensitive attributes	Measure the distance between two probabilistic distributions	prone to skewness

3. Proposed System

The proposed system generates privacy preserved text document summary which uses sensitivity context aware anonymization which is a machine learning-based approach focused on unstructured text data. It is mainly described in Figure.1, where the raw text documents are fed as input and are subjected to domain-specific extensive focuses on sensitivity context which is varied from one domain to another. The proposed system architecture is natural language pre-processing processes before the document classification due to the unstructured nature of extractive summarization extracts

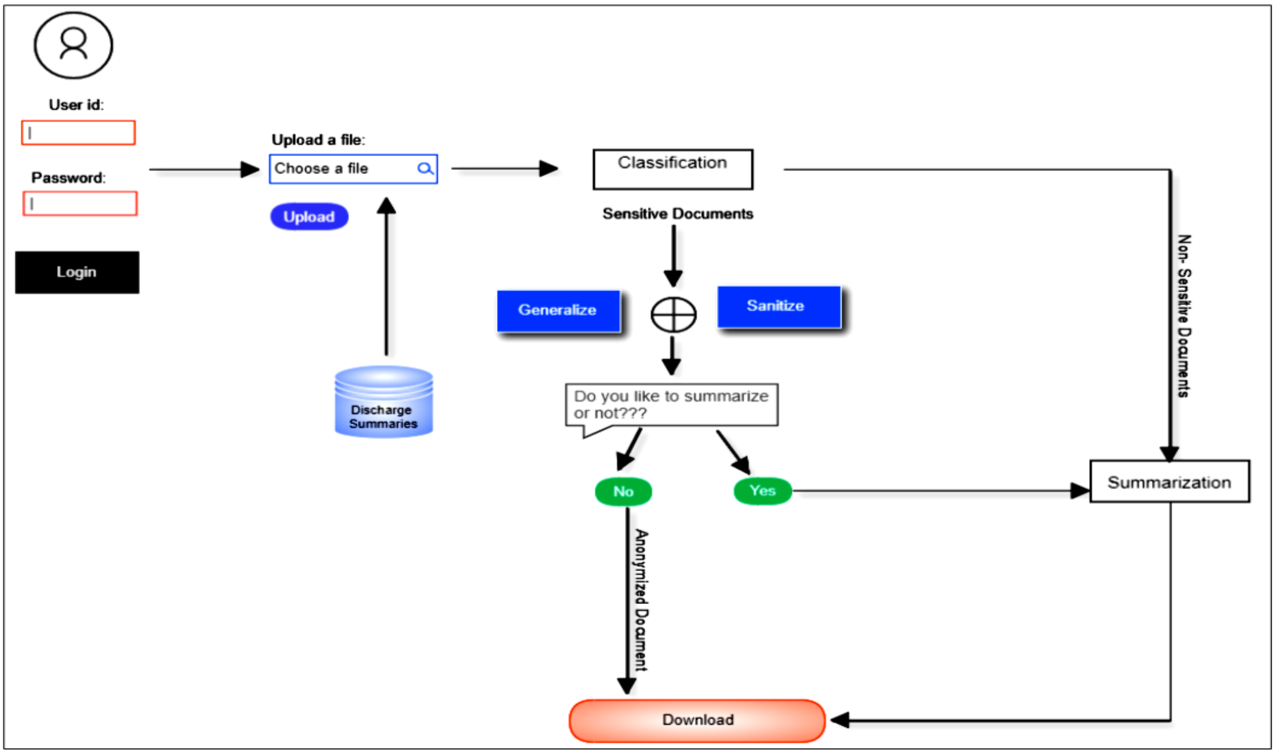


Figure 1: System Architecture of Privacy Preserving Document Summary Generation

a subset of words from a document which treated as most important and specific to the domain to create a single specific summary pertaining to a document. In extractive summarization, weightage is assigned to vital sections of sentences.

Diverse methods and approaches can be used to instrument the sentence weight. Sentence joining is done with relevance and resemblance to domain context to produce a summary. The main features used to generate an extractive summary from patient discharge summary are the past medical history and disease medications on admission related to a particular patient. The discharge summary mainly contains patient individual and disease-specific characteristics as words, sentences, or paragraphs. After preprocessing of discharge summaries, the patient characteristics are available as tokens i.e., words. The sensitive words are those which are identified w.r.t. sensitivity context i.e., determined from the healthcare organization perspective and patients. The sensitivity context required for model development is implemented using a lexicon. It is the knowledge base such that the words in the lexicon are treated as sensitive features which are decided based on the patient's disease details and organizational data regulations. The different phases of the proposed system are as follows:

- Classification-The input text document is classified into a sensitive document or not-sensitive document based on the healthcare domain knowledge and sensitive attributes like disease type present in the given input document.
- Sanitization-This module takes the sensitive document as input and anonymizes the document partially by replacing it with Synthetic data. Generalization- This module takes the sensitive document as input and anonymizes the document completely by replacing it with generic data.
- Summarization- Summarization is the process of highlighting medical information which helps the medical experts efficiently identify the records. The patient's Discharge Summary is given as an input file.

The text document is classified into sensitive or not-sensitive based on the medical terminologies associated with the healthcare domain like sensitive drugs, diseases, etc present in it. The sensitive documents are sent to the anonymization process which is based on the user consent and the anonymization done in two ways they are Generalization and Sanitization. In Generalization, the document is anonymized completely by replacing the quasi attribute with generic data relevant to the healthcare domain. In Sanitization, a document is anonymized partially by replacing the quasi attributes with synthetic data. The anonymized document is subjected to summarization based on the user's choice of whether they are interested to generate a summary or not. If not, then the output document will be either a generalized document or sanitized document. The not-sensitive document is Suppressed, where the Personally Identifiable Information (PII) such as the patient's name, phone number, etc. is suppressed and forwarded to the Summarization process. The input text document is classified into a sensitive document or not-sensitive document based on the sensitive attributes such as diseases present in the given document [10], [11].

Multinomial Naive Bayes and Logistic Regression Supervised classification techniques are used to predict the target label for the text document as sensitive or not sensitive based on the sensitivity context. Multinomial Naive Bayes is a popular probabilistic classifier based on Bayes Theorem. It uses probability to determine the label of a text grounded on prior knowledge of conditions. It calculates the probability of each tag which is further assigned for a given text and performs label prediction for the tag with the highest probability. Equation 1 describes posterior probability computation to perform the classification of documents based on sensitivity context.

$$P(U|V) = \frac{\mathrm{P(V|U)\ P(V)}}{P(U)} \qquad (1)$$

where P(U|V) represents the posterior probability of U existence is True with a certain V is True, P(V|U) represents the maximum likelihood of U existence is True certain V is True, P(U) is the prior probability of U existence is true and P(V) is a marginalization of probability V existence is True.

In this approach, to break the sentences as n-grams, the NLTK n-gram tokenizer module is used. The resultant tokens are considered features and the most frequent features are nominated to each predefined class. A feature set is constructed with the union of features that are nominated to predefined classes. The sensitive terms are represented as bag-of-words i.e., a vector $xi = \{xi_1, xi_2, xi_3, \ldots, xi_n\}$, where xi is the number of times the vocabulary term appears in the text document. MNB classifies documents as sensitive or not sensitive based on the posterior probability of the terms with their label occurrence It is determined either by referring to actual sensitive content or consent about data disclosure from an individual patient [12].

Logistic regression is a binary classifier that performs prediction when the target variable is categorical. The Logistic Regression classifier estimates categorical dependent variable relationship with other independent variables and uses binary values of the dependent variable. Logistic Regression refers to predicted values probability scores that are related to the dependent variables i.e., sensitive terms in a range between 0 to 1 & also consider dependent variable natural logs of odds to find refined dependent variable by referring to a logit function. The value nearer to 1 is labeled as a sensitive document otherwise value nearing 0 is labeled as a not sensitive document. In the proposed approach a threshold value of 0.50 is used as a prediction threshold. The odds ratio determines the ratio of success to failure and the same is described in "(2)" where P is the probability of sensitive term occurrences in a document and 1-P is the probability of not occurring of sensitive terms in a document and $0 \leqslant O \leqslant \infty$.

$$O = \frac{P}{1-P} \qquad (2)$$

$$\mathrm{Y(1|0) = b + w_i X_i} \qquad (3)$$

The predicted label Y is categorical and dependent on the independent variables and its co-efficient which is given in "(3)" where $-\infty \leqslant Xi \leqslant \infty$. The logit function is used to predict outcomes as a sensitive document or not sensitive document. The logit function depends on the probability of feature occurrences P and it is 0 < Pi < 1. Equation (4) and Equation(5) describes the prediction of the test record label as sensitive or not sensitive where, 0 < Pi < 1 [13].

$$\mathrm{Logit(Pi)} = \ln(\frac{\mathrm{Pi}}{1-\mathrm{Pi}}) = f(x) \qquad (4)$$

$$\mathrm{Pi} = \frac{e^{f(x)}}{1+e^{f(x)}} \qquad (5)$$

The sanitization approach takes the sensitive document as input and anonymizes the document partially by replacing it with synthetic data. Synthetic data is the artificial data created by the programmer to preserve the privacy of personal information. Explicit Identifiers are extracted and removed, whereas Quasi Identifiers are extracted and replaced with synthetic data. Feature Extraction is carried out using Regular Expressions which are specific to the healthcare domain [14], [15]. In generalization, both explicit identifiers and quasi-identifiers are extracted. Explicit Identifiers are extracted and removed. Quasi Identifiers are extracted and replaced with generic data. Extraction is carried out using Regular Expressions which are specific to the domain [16] Table 2 describes how the quasi attributes in a sensitive document are anonymized using the proposed approach. In suppression, the explicit identifiers present in the not-sensitive documents are extracted and later suppresses by replacing them with predefined non-readable characters[17], [18]. Summarization is the process of highlighting medical information which helps the medical experts to identify records efficiently. Extractive summaries are created by borrowing phrases or sentences from the original input text [19]. The summarized document in which clinical terms such as dosage, drugs, duration, and frequency of medicine intake are mentioned. For better visual appearance medication strengths are highlighted. The outcome of the proposed approach is described in Figure 2. The text document segmentation breakdown a lengthy document into a shorter one. Shorter segments are sometimes dependent on grammatical rules or dependent on topic continuousness. The term frequency-inverse document frequency-based sentence weightage is used which helps to discriminate and add important domain requirement-specific aspects in the generated summary. The normalized frequency weights approach is used to discriminate repeated words in a specific document and from a generic corpus which may also contain stop words. To overcome it background information about the healthcare domain is used at the time of stop word removal. The stop word lists are used to eliminate the irrelevant words [20].

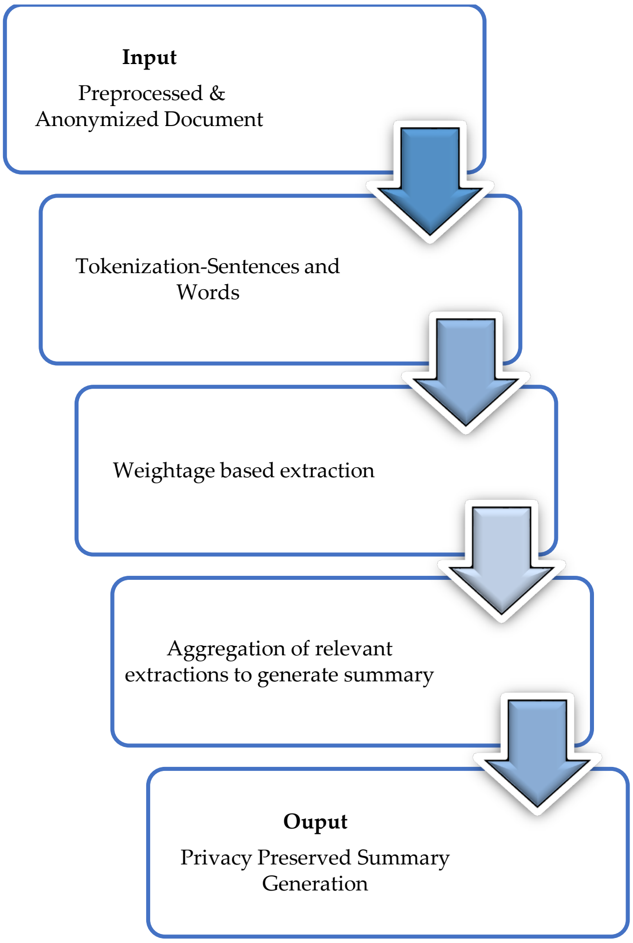

Input
Preprocessed & Anonymized Document
Tokenization-Sentences and Words
Weightage based extraction
Aggregation of relevant extractions to generate summary
Ouput
Privacy Preserved Summary Generation

Figure 2: Privacy Preserving Summary Generation Process

The term weightage is approximated using the product of term frequency and inverse document frequency. The inverse document frequency normalization is used to determine the weightage. Let Y = (y1, . . . , yd) be the terms in a document, and idfk is the kth term inverse document frequency. The weight wk can be calculated using "(6)" where the product of terms y_k and *idf_k* inverse document frequency weight is divided by maximum word frequency outcome is used for document normalization[21], [22].

$$w_k = \frac{y_k \cdot idf_k}{max\{y_i \cdots y_d\}} \tag{6}$$

Terms with weight wk below is a certain threshold is set to weight value 0 and they are treated as not important terms. wk used to score the sentences. The average weight of words related to sentence Sr is used to calculate sentence significance. Average weight µw(Sr) of word w.r.t sentence Sr calculation described in " (7)".

$$\text{Avg. Weight(Sr)} = \frac{\sum_{tk\in Sr} wk}{|\{t:tk\in Sr\}|} \tag{7}$$

Sentences are sorted in descending order w.r.t. to calculated weightage. The sentences with a higher score are selected to produce a summary. Sentence selection for summary generation is dependent on the scoring approach used and the possibility of pairing different selection methods with different scoring methods. Table.2 describes the anonymization of sensitive quasi attributes related to patients in the discharge summary before the summary generation. Sensitive quasi attributes anonymization mainly depends on the domain requirements and consent from the patients regarding the data disclosure [23], [24].

Quasi Identifiers in the discharge summary documents are either hidden or removed based on the type of privacy required by the user. Then for visual representation only the essential text data is extracted and displayed, hence it preserves the privacy of the individual. Algorithm-1 and Algorithm-2 describe procedures associated with the proposed system development.

4. Results and Discussions

The summarization needs to find the important sections of the discharge summary. The summarization assessment can be done using content evaluation. In content evaluation, thoughts of the original document are available in the produced summary which is in turn relevant to human expert generated summary i.e., an ideal summary is analyzed. The Summarization assessment can be done using content evaluation. In content evaluation, thoughts of the original document are available in the produced summary which is in turn relevant to human expert generated summary i.e., an ideal summary is analyzed. Compression Rate (CR), Precision (P), and Recall (R) metrics are used to evaluate the generated summary and the same described in "(8)", "(9)" and "(10)".

Algorithm 1: Privacy Preserving Hospital Discharge Report Generation.

```
Input: Patient Discharge Summary Document.
Output: Patient Privacy preserved and summarized discharge summary document.

1. Preprocess discharge summary documents.
2. Collect the consent about sensitive data disclosure from the user.
for all preprocessed discharge summary documents do
    Classify documents as sensitive /not-sensitive based on disclosure consent from the user;

    if a document is sensitive then
        Prompt user for sanitization or generalization.
        Generate summary;
    else not-sensitive document then
        Apply suppression.
        Generate summary;
    end
end
```

$$CR = \frac{\text{automated summary length}}{\text{length of the actual document}} \quad (8)$$

$$P = \frac{\text{sentences in system summary+sentences in ideal summary}}{\text{system summary overall sentences}} \quad (9)$$

$$R = \frac{\text{sentences in system summary+sentences in ideal summaries}}{\text{ideal summary overall sentences}} \quad (10)$$

Table 2: Sensitive Quasi attributes Anonymization

Generic Data	Anonymized Data
Name: Mr. John → [NAME] (Entity name)	Name: Mr. John → [NAME] (Entity name)
Age: 43 years → [40-50] years (range)	Age: 43 years → [45.5] years (binning average)
Date: 12-03-2006 → [DATE]	Date: 12-03-2006 →[2006] (year)
Record Identifier 13456	Identifier ##### Suppressed data

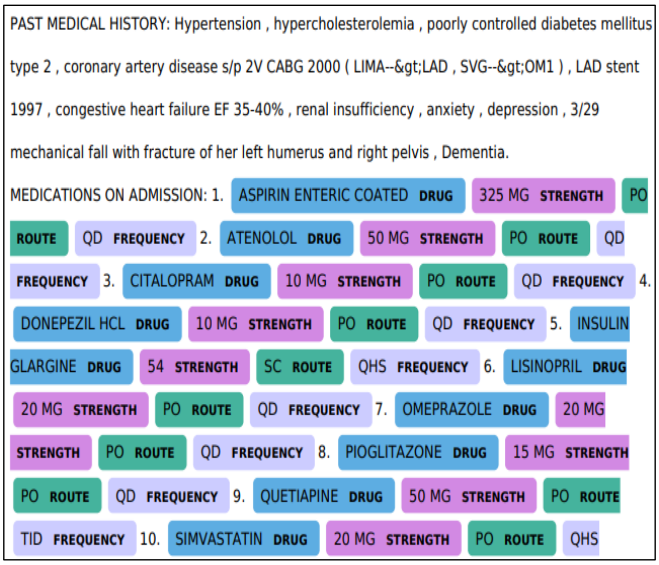
Algorithm 2: Privacy Preserving Document Summarization.

```
Input: Anonymized Document.
Output: Summarized Document.
    1. Identify the labels of interest related to the
       requirement domain.
    2. Store domain-specific keywords in a list.
    3. Initialize word dictionary WD.
    4: Initialize sentence dictionary SD.
    5: initialize sentence score dictionary SSD.
for all the anonymized discharge summary documents do
    Sentence tokenization.
    Word Tokenization;
    if a sentence is not in SD then
        SD[sentence]= WD[word]
    else
        SD[sentence]+= WD[word];
    end
end
6.generate histogram with sentence weight
for k exists in WD do
    WD[k]=WD[k]/maximum(WD.values());
end
7. generate summary w.r.t highest sentence score
```

The i2b2 data set used for experimentation consists of discharge summaries which have the following details particular to each patient and they are Disease victim or Patient-Attributes

- Reason for admission
- Past medical history
- Medication on admission
- Significant discoveries
- Procedures and treatment offered.
- Patient's discharge state
- Instructions to Patient/family
- Physician's details – one who attends patient during treatments.

Figure 3 shows only the required details like a past medical history of a patient in the generated summary and details of drugs used in the patient medication are highlighted in colors.



PAST MEDICAL HISTORY: Hypertension , hypercholesterolemia , poorly controlled diabetes mellitus type 2 , coronary artery disease s/p 2V CABG 2000 (LIMA--&gt;LAD , SVG--&gt;OM1) , LAD stent 1997 , congestive heart failure EF 35-40% , renal insufficiency , anxiety , depression , 3/29 mechanical fall with fracture of her left humerus and right pelvis , Dementia.

MEDICATIONS ON ADMISSION: 1. ASPIRIN ENTERIC COATED DRUG 325 MG STRENGTH PO ROUTE QD FREQUENCY 2. ATENOLOL DRUG 50 MG STRENGTH PO ROUTE QD FREQUENCY 3. CITALOPRAM DRUG 10 MG STRENGTH PO ROUTE QD FREQUENCY 4. DONEPEZIL HCL DRUG 10 MG STRENGTH PO ROUTE QD FREQUENCY 5. INSULIN GLARGINE DRUG 54 STRENGTH SC ROUTE QHS FREQUENCY 6. LISINOPRIL DRUG 20 MG STRENGTH PO ROUTE QD FREQUENCY 7. OMEPRAZOLE DRUG 20 MG STRENGTH PO ROUTE QD FREQUENCY 8. PIOGLITAZONE DRUG 15 MG STRENGTH PO ROUTE QD FREQUENCY 9. QUETIAPINE DRUG 50 MG STRENGTH PO ROUTE TID FREQUENCY 10. SIMVASTATIN DRUG 20 MG STRENGTH PO ROUTE QHS

Figure 3: Summarized Medical History and Medicine prescription

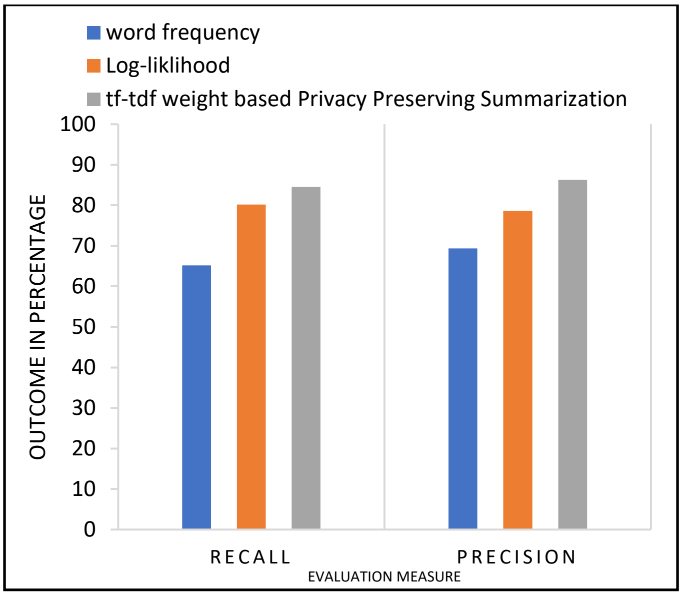


Figure 4: Evaluation of privacy preserving text document Summarization

The proposed approach uses tf-idf-based feature selection to generate the privacy preserved summary. It achieves better results when compared with word frequency where how many times a required word appears in the document sections without referring to sensitivity context. It performs well when compared to log-likelihood topic selection approaches where it requires a sample summary that contains the required terms and relevant terms probability distributions without referring to sensitivity context. The proposed approach compared against word frequency-based and log likelihood-based summarization approaches are described in Figure 4.

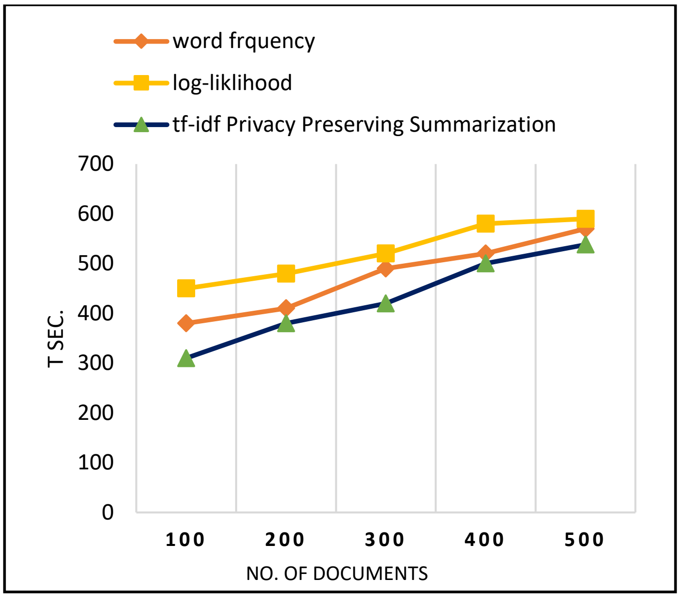


Figure 5: tf-idf based summarization computational analysis.

The proposed approach also generates a summary in a lower computational time since it has already classified the documents based on sensitivity context which is an automated process and not sensitive documents are directly subjected to summarization. When compared to word frequency and log-likelihood topic selection approaches where sensitivity context based selection and classification is not used. The computational evaluation of the proposed approach is described in Figure 5.

5. Conclusion

The proposed approach preserves the privacy of patients whose details are available in the discharge summary as unstructured text data. Extensive domain-specific text pre-processing is required prior to the privacy preserved summary generation. The proposed approach uses a classification technique to initially categorize the discharge summary document based on sensitivity context. The results indicate that the proposed tf-idf-based summarization computationally performed well when compared with other summarization techniques. It also preserves patient privacy without defying privacy constraints.

Acknowledgments

The corpus used in the proposed research work is from the Informatics for Integrating Biology and Bedside Organization, Harward University, USA. Each Discharge summary is unique to a patient, and it consists of patient disease-specific treatment procedures It contains cardiac, diabetes, and tuberculosis patient discharge summaries.

References

[1] K. P. Ramya Shree A N, RNSIT, “Privacy preserving data mining on unstructured data,” *International Conference on Science, Technology, Engineering and Management (ICSTEM'17)*, vol. 2, no. 2, 2017.

[2] A. N. R. Shree, P. Kiran, “Sensitivity Context Aware Privacy Preserving Text Document Summarization,” *Proceedings of the 4th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2020*, pp. 1517–1523, 2020, doi:10.1109/ICECA49313.2020.9297415.

[3] K. P. Ramya Shree A N, “Privacy Preserving Unstructured Data Publishing (PPUDP) Approach for Big Data,” *International Journal of Computer Applications*, vol. 178, no. 28, pp. 4–9, 2019, doi:10.5120/ijca2019919091.

[4] A. N. R. Shree, P. Kiran, “Quasi Attribute Utility Enhancement (QAUE) - A Hybrid Method for PPDP,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075*, vol. 9, no. 2S, pp. 330–335, 2019, doi:10.35940/ijitee.B1087.1292S19.

[5] F. Dernoncourt et al., “De-identification of patient notes with recurrent neural networks,” *Journal of the American Medical Informatics Association*, vol. 24, no. 3, pp. 596–606, 2017, doi:10.1093/jamia/ocw156.

[6] V. T. Chakaravarthy et al., “Efficient techniques for document sanitization,” *International Conference on Information and Knowledge Management, Proceedings*, pp. 843–852, 2008, doi:10.1145/1458082.1458194.

[7] B. Gedik, L. Liu, “A Customizable k-Anonymity Model for Protecting Location Privacy,” (Springer, 2004), 620–629, doi:https://doi.org/10.1007/978-981-16-9012-9_49.

[8] K. LeFevre, D. J. DeWitt, R. Ramakrishnan, “Incognito: Efficient full-domain K-anonymity,” *Proceedings of the ACM SIGMOD*

International Conference on Management of Data, pp. 49–60, 2005, doi:10.1145/1066157.1066164.

[9] T. Christensen, A. Grimsmo, "Instant availability of patient records, but diminished availability of patient information: A multi-method study of GP's use of electronic patient records," *BMC Medical Informatics and Decision Making*, vol. 8, pp. 1–8, 2008, doi:10.1186/1472-6947-8-12.

[10] R. S. K, "A New Efficient Cloud Model for Data Intensive Application," *Global Journal of Computer Science and Technology*, vol.15,no.1,pp.19–30,2015, doi:https://computerresearch.org/index.php/computer/article/view/1135.

[11] A. N. Ramya Shree, P. Kiran, S. Chhibber, "Sensitivity Context-Aware PrivacyPreserving Sentiment Analysis," *Smart Innovation, Systems and Technologies*, vol. 213 SIST, pp. 407–416, 2021, doi:10.1007/978-981-33-4443-3_39.

[12] A. Majeed, S. O. Hwang, "A Comprehensive Analysis of Privacy Protection Techniques Developed for COVID-19 Pandemic," *IEEE Access*, vol. 9, pp. 164159–164187, 2021, doi:10.1109/ACCESS.2021.3130610.

[13] E. K. Lee, K. Uppal, "CERC: an interactive content extraction, recognition, and construction tool for clinical and biomedical text," *BMC Medical Informatics and Decision Making*, vol. 20, no. Suppl 14, pp. 1–14, 2020, doi:10.1186/s12911-020-01330-8.

[14] M. R. Naqvi et al., "Importance of Big Data in Precision and Personalized Medicine," *HORA 2020 - 2nd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*, pp. 2–7, 2020, doi:10.1109/HORA49412.2020.9152842.

[15] N. K. Anuar, M. Uniten R&D Sdn. Bhd., Kajang, Selangor, ; Asmidar Abu Bakar; Aishah Abu Bakar, "No Title," *2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP)*, no. 6, pp. 1048–1052, 2021, doi:https://doi.org/10.1109/ICSIP52628.2021.9688624.

[16] C. C. Aggarwal, P. S. Yu, "A General Survey of Privacy-Preserving Data Mining Models and Algorithms," pp. 11–52, 2008, doi:10.1007/978-0-387-70992-5_2.

[17] A. N. R. Shree, P. Kiran, "Sensitivity Context Awareness based Privacy Preserving Recommender System," *SSRN Electronic Journal*, no. Icicc, pp. 1–5, 2021, doi:10.2139/ssrn.3835011.

[18] Kiran P A N Ramya Shree, "SCAA—Sensitivity Context Aware Anonymization—An Automated Hybrid PPUDP Technique for Big Data," in *Sustainable Advanced Computing*, ed S.K Aurelia, S., Hiremath, S.S., Subramanian, K., Biswas (Singapore: Springer Nature, 2022), 615–626, doi:https://doi.org/10.1007/978-981-16-9012-9_49.

[19] B. B. Mehta, U. P. Rao, "Privacy Preserving Unstructured Big Data Analytics: Issues and Challenges," *Physics Procedia*, vol. 78, pp. 120–124, 2016, doi:10.1016/j.procs.2016.02.020.

[20] A. El Haddadi et al., "Mining unstructured data for a competitive intelligence system XEW," *SIIE 2015 - 6th International Conference on "Information Systems and Economic Intelligence,"* pp. 146–149, 2015, doi:10.1109/ISEI.2015.7358737.

[21] A. Bafna, J. Wiens, "Automated feature learning: Mining unstructured data for useful abstractions," *Proceedings - IEEE International Conference on Data Mining, ICDM*, vol. 2016-Janua, pp. 703–708, 2016, doi:10.1109/ICDM.2015.115.

[22] P. Jain, M. Gyanchandani, N. Khare, "Big data privacy: a technological perspective and review," *Journal of Big Data*, vol. 3, no. 1, 2016, doi:10.1186/s40537-016-0059-y.

[23] X. Wu et al., "Privacy preserving data mining research: Current status and key issues," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4489 LNCS, no. PART 3, pp. 762–772, 2007, doi:10.1007/978-3-540-72588-6_125.

[24] C. Zhang et al., "Automatic keyword extraction from documents using conditional random fields," *Journal of Computational Information Systems*, vol. 4, no. 3, pp. 1169–1180, 2008.

Ms. A N Ramya Shree has done her bachelor's degree from KVGCE institution in 2005. She has done her master's degree from SJBIT institution in 2010. The author has a total of 16 + Years of Academic and Research experience. Her research interests include Privacy Preserving Data Publishing and Natural Language Processing. She received the "Predictive Analytics Modeler - Explorer Award 2020" badge by IBM Bengaluru in 2020. She has presented and published a total of 12 research papers in reputed international conferences and journals.

Dr. P Kiran has done his bachelor's degree from AIT institution in 2000. He had done his master's degree from SJCE institution in 2003. He completed his Ph.D. degree in Computer Science from Visvesvaraya Technological University in 2014. The author has a total of 20 + Years of Academic and Research experience. His research interests include Cryptography, Randomization, Anonymization methods in Generalization, Indexing techniques, and Design Patterns. He has presented and published 40+ research papers in reputed international conferences and journals.

Received: 15 March 2022, Revised: 20 June 2022, Accepted: 23 June 2022, Online: 18 July 2022

DOI: https://dx.doi.org/10.55708/js0107003

Impact of Gender of Lecturers' on Learning among the College of Arts and Commerce Students' at Andhra University

Gordon Amidu*

Department of Library and Information Science, Andhra University, Visakhapatnam- Andhra Pradesh, 530003, India
* Corresponding author: Gordon Amidu, gordonamidu40@ymail.com, +917075324651

ABSTRACT: The purpose of this study was to determine Impact of Gender of Lecturers' on Learning among the College of Arts and Commerce Students' at Andhra University. Systematic data collection and analysis efforts resulted in the following findings: A question was presented to find out which lecturer gender produces difficult examination questions. According to the findings, 74 (51.4%) of respondents stated it was mostly male lecturers, 56 (38.9%) said it was a balance of male and female lecturers, and 15 (10.4%) said it was female lecturers. Again, Students were asked a question to determine which lecturer gender teaching styles they liked. According to the findings, 47 (32.6%) of respondents chose male lecturers, 34 (23.6%) preferred female lecturers, and the majority of respondents 63 (43.8%) preferred both male and female lecturers. Furthermore, Students were asked a question to determine which lecturer gender they preferred. According to the findings, 54 (37.5%) of respondents chose male lecturers, 27 (18.8%) preferred female lecturers, and the majority of respondents 64 (44.4 %) preferred both male and female lecturers. Finally, Students were asked a question to determine which lecturer gender they feel most comfortable approaching. According to the findings, 40 (27.8%) of respondents chose female lecturers, 49 (34%) preferred male lecturers, and the majority of respondents 55 (38.2%) preferred both male and female lecturers. Suggestions were made to establish an effective and conducive teaching atmosphere between lecturers and students at Andhra University College of Arts and Commerce.

KEYWORDS: Evaluating lecturers, Teaching skills, Gender of lecturers

1. Introduction

Gender is a sociological concept that is used to define social distinctions between men and women and from which these differences can be deduced [1]. Gender inequality in the workplace is equated with inequalities between men and women on a number of levels: women are employed in "female" positions as opposed to men who are hired in "masculine" ones, income levels, the number of women holding crucial positions, and more [2]. Gender stereotypes exist as well, and are defined as "common, rigid, and generalised patterns of thought that ascribe to men and women characteristics, personal qualities, and behaviours that are attributed to their biological gender and that do not take into account any individual reality" [3], [4]. Stereotypes cause individuals to attribute to men the qualities and functions associated with the male stereotype and to women the attributes associated with the feminine stereotype [5], [6].

Education is a process that assists future generations in acquiring new knowledge and improving their character, literacy, and abilities. It is the guiding principle for the growth of communities all around the world. Teaching, on the other hand, is a process in which one individual leads others in developing their talents and literacy. It is seen as a key action in the process of transferring knowledge to students [7], [8]. The lecturer, defined here as a professional or academic specialist working in higher education institutions who assists students in the learning process, is one of the most powerful variables influencing teaching and learning [9]. In a learning environment, lecturers' behaviour is critical in assisting students to attain the intended learning goals of their courses or programmes

[10]. Students' experiences at educational institutions can be strongly influenced by their lecturers' behaviours, even to the point where these behaviours may have an impact on students' learning results [11]. In general, lecturers' main behavioural tendencies include a punishing, rewarding, accommodating, criticising, or requiting approach [12]. It is thus imperative to study whether there is a link between the gender of lecturers and learning among students in the College of Arts and Commerce, particularly at Andhra University.

The answers to these essential questions would form solutions to this study's problem statement.

2. Problem Statement

There are various schools of thought regarding the effect of lecturer gender on student accomplishment. Some schools of thought contend that lecturer gender has no effect on student accomplishment, but others contend that lecturer gender has an effect on student achievement. This study was conducted at Andhra University’s College of Arts and Commerce to elicit students’ opinions on the impact of lecturers' gender on learning.

3. Study Objectives

The main objective of this study is to assess students' viewpoints on the impact of lecturers' gender on learning among students in the college of arts and commerce at Andhra University.

The study specifically seeks to;

1. To find out the general students opinion of lecturers' gender
2. Examine the relationship between lecturers' gender and the perceived difficulty of examination questions.
3. Assess students' perceptions of their lecturers' gender, as well as their teaching approaches and methods.
4. Study the relationship between the gender of the student and the gender of the preferred lecturers.
5. Examine the connection between lecturer gender and student participation in class.

The answers to these essential objectives would form solutions to this study's problem statement.

4. Literature Review

According to [13], female instructors in elementary and middle schools outperform their male counterparts in terms of enhancing both male and female student achievement. The benefits of having female math teachers are especially significant for female students' arithmetic achievement, but they found no indication of a beneficial gender matching impact in English language arts. Furthermore, contrary to popular belief, males do not perform better academically when allocated to male teachers. Their findings indicated that the impacts of instructor gender on student learning differed depending on subject and gender, but the effect sizes were negligible.

According to [14], research on Gender stereotyping in student perceptions of teaching excellence: adopting the changing standards hypothesis. Chi-square tests found that gender had a substantial impact on the distribution and thematic content of submissions. The findings indicated that students were more likely to nominate teachers of the same gender, but that male students were proportionally less likely to nominate a female teacher. Gender biases pervade student perceptions of TE, particularly among male students. These findings suggest that students' judgments of high-quality instruction are inextricably linked to societal influences.

In [15], the author did a study titled: Does professors' gender effect how students perceive their teaching and suggestions for the best professor? The study revealed that when undergraduates rated their professors on certain criteria related to teaching performance, they shared their opinions independently of the professors' gender. When asked for a single overall judgement, such as whether they would suggest the professor as one of their greatest instructors, students favoured male professors over their female classmates by a modest margin.

According to [16], most respondents felt that male lecturers were favoured over females because they improved academic achievement, which is consistent with the study's findings that ranked male lecturers somewhat higher than female lecturers. However, the majority of respondents believed that a lecturer's gender did not matter, which was consistent with the reviewed literature. Other factors they said were more essential included course mastery, lecturing style, sincerity of student and interest in course, personality of lecturer, and lectures would be more impactful if class number was reduced. Others agreed that both male and female lecturers were good, and that they each had their strengths; ladies were stricter and more authoritative, while men were more tolerant. Female instructors received mostly unfavorable feedback, with some claiming that they do not assign grades and have a bad impact on students. Others agreed that both genders were good, although male lecturers had a little higher rating. "Both genders are good, but male has a greater favourable impact," they said. Others believed that the gender of lecturers had an impact on both teaching and learning.

In [17], the author conducted a study on the Influence of Gender and Age of Teachers on Teaching: Students' Perspective, which revealed that most students did not see gender or age as a barrier in teaching until the teacher was active and interested in teaching, and they believed that experience had a positive influence on teaching. Females, on the other hand, preferred females because they thought it was easier to communicate with them. Many students believed that females are kind, diligent, truthful, and had a high-pitched voice that is audible.

In [18], the author discovered that male secondary school students in the Segamat district aspired to be engineers, businessmen, or entrepreneurs. Female students, on the other hand, preferred careers such as teachers, lecturers, and accountants. As a result, the best male students picked engineering programmes offered by local colleges, while the rest pursued alternative fields such as accounting. The best female students enrolled in university programmes such as accounting in order to become teachers/lecturers or accountants.

5. Methodology

To collect information, a survey method was used. A well-structured questionnaire was created to elicit feedback from the College of arts and commerce students at Andhra University. A total of 250 questionnaires were distributed, with 146 duly completed questionnaires returned, resulting in a response rate of 58.4 %. The respondents were asked to select the most appropriate answer from a list of possible answers, and the data was tabulated and analyzed.

6. Results and Analysis

6.1. Gender breakdown of the responses

The table 1 shows that of the 143 responses, 103(72 %) are male, 40(28 %) are female and 0(0%) representing other gender. This demonstrates that male sample is more in Andhra University's College of Arts and Commerce.

6.2. Status-wise distribution of responses.

Table 2 depicts the distribution of respondents based on their status. According to the table, the majority of respondents, 105 (72.9%), are postgraduate students, followed by 26 (18.1 %) who are PhD students, and the least, 13 (9 %), are undergraduates. The table clearly reveals that postgraduate students make up the vast majority of respondents.

Table 1: Responses gender distribution

Gender	Number of respondents	Percentage
Male	103	72%
Female	40	28%
Other	0	0%

Table 2: Status-wise distribution of responses

Status	Number of respondents	Percentage
Postgraduate	105	72.9%
Undergraduate	13	9%
PhD	26	18.1%

6.3. Age-wise distribution of responses

Table 3 depicts the distribution of respondents based on their age. According to the table, the majority of respondents are between the ages 20-25, (83(58.5%), followed by those between the ages 25-30, (48 (33.8 %) and the least between the ages 35-40, (11(7.7%). This demonstrates that the majority of students at the College of Arts and Commerce are postgraduates between the ages of 20 and 25.

Table 3: Age-wise distribution of responses

Status	Number of respondents	Percentage
Postgraduate	105	72.9%
Undergraduate	13	9%
PhD	26	18.1%

6.4. To Examine the relationship between lecturers' gender and the perceived difficulty of examination questions.

A question was presented to find out which lecturer gender produces difficult exam questions. According to Table 4, 74 (51.4%) of respondents stated it was mostly male lecturers, 56 (38.9%) said it was a balance of male and female lecturers, and 15 (10.4%) said it was female lecturers.

Table 4: to Examine the relationship between lecturers' gender and the perceived difficulty of examination questions.

Status	Number of respondents	Percentage
Postgraduate	105	72.9%
Undergraduate	13	9%
PhD	26	18.1%

6.5. To assess students' perceptions of their lecturers' gender, as well as their teaching approaches and methods

Students were asked a question to determine which lecturer gender teaching styles they liked. According to Table 5, 47 (32.6 %) of respondents chose male lecturers, 34

(23.6 %) preferred female lecturers, and the majority of respondents 63 (43.8 %) preferred both male and female lecturers.

Table 5: to assess students' perceptions of their lecturers' gender, as well as their teaching approaches and methods

Status	Number of respondents	Percentage
Postgraduate	105	72.9%
Undergraduate	13	9%
PhD	26	18.1%

6.6. *To study the relationship between the gender of the student and the gender of the preferred lecturer*

Students were asked a question to determine which lecturer gender they prefer. According to Table 6, 54 (37.5%) of respondents chose male lecturers, 27 (18.8%) preferred female lecturers, and the majority of respondents 64 (44.4 %) preferred both male and female lecturers.

Table 6: to study the relationship between the gender of the student and the gender of the preferred

Status	Number of respondents	Percentage
Postgraduate	105	72.9%
Undergraduate	13	9%
PhD	26	18.1%

6.7. *To examine the approachable nature of the lecturer based on gender*

Students were asked a question to determine which lecturer gender they feel most comfortable approaching. According to Table 7, 40 (27.8%) of respondents chose female lecturers, 49 (34%) preferred male lecturers, and the majority of respondents 55 (38.2%) preferred both male and female lecturers.

Table 7: to examine the connection between lecturer gender and student participation in class

Status	Number of respondents	Percentage
Male	49	34%
Female	40	27.8%
Both	55	38.2%

7. Findings

The following are the findings as a result of systematic data gathering and analysis efforts:

A question was presented to find out which lecturer gender produces difficult examination questions. According to Table 4, 74 (51.4%) of respondents stated it was mostly male lecturers, 56 (38.9%) said it was a balance of male and female lecturers, and 15 (10.4%) said it was female lecturers. The findings clearly reveal that male lecturers at Andhra University's College of Arts and Commerce ask difficult examination questions.

Students were asked a question to determine which lecturer gender teaching styles they liked. According to Table 5, 47 (32.6 %) of respondents chose male lecturers, 34 (23.6 %) preferred female lecturers, and the majority of respondents 63 (43.8 %) preferred both male and female lecturers. The findings clearly show that students preferred the teaching techniques of both male and female lecturers at Andhra University's College of Arts and Commerce.

Students were asked a question to determine which lecturer gender they prefer. According to Table 6, 54 (37.5%) of respondents chose male lecturers, 27 (18.8%) preferred female lecturers, and the majority of respondents 64 (44.4 %) preferred both male and female lecturers. The facts clearly reveal that students liked both male and female teachers at Andhra University's College of Arts and Commerce.

Students were asked a question to determine which lecturer gender they feel most comfortable approaching. According to Table 7, 40 (27.8%) of respondents chose female lecturers, 49 (34%) preferred male lecturers, and the majority of respondents 55 (38.2%) preferred both male and female lecturers. The facts clearly show that students at Andhra University's College of Arts and Commerce felt more comfortable approaching both male and female teachers, followed by male lecturers, and finally female lecturers.

8. Recommendations

Male lecturers should be a little more flexible when it comes to setting exam questions so that students feel less nervous while taking exams.

In order to achieve gender balance in terms of academics, Andhra University should appoint both male and female teaching staff on the basis of merit.

Lecturers should be more approachable and friendly to students so that they can approach them and share their academic concerns.

9. Conclusion

According to the findings, male lecturers at Andhra University's College of Arts and Commerce undoubtedly pose difficult examination questions. According to the study, students at Andhra University's College of Arts and Commerce preferred both male and female lecturers' teaching styles. Furthermore, the findings clearly reveal that both male and female lecturers were well-liked by students. Finally, the findings show that students at Andhra University's College of Arts and Commerce felt more comfortable approaching both male and female teachers, however male lecturers were slightly more preferred than female counterparts. The majority of respondents responded that the gender of a lecturer made no impact, which was consistent with the reviewed literature. Respondents also believed that other variables that were more essential to them included course expertise, lecturing style, student honesty, and passion for the course, all of which are critical to positively influence students' success.

Conflict of Interest

The author declares no conflict of interest.

References

[1] N. Raz, K. M. Rodrigue, "Differential aging of the brain: Patterns, cognitive correlates and modifiers," *Neuroscience and Biobehavioral Reviews*, vol. 30, no. 6, pp. 730–748, 2006, doi:10.1016/j.neubiorev.2006.07.001.

[2] C. D. Bodhe, D. S. Jankar, "Teaching effectiveness: how do students evaluate their teacher?," *International Journal of healthcare and Biomedical Research*, vol. 63, no. 2, pp. 155–459, 2015.

[3] F. Ochsenfeld, "The gender income gap and the role of family formation revisited," *Journal for Labour Market Research*, vol. 50, no. 1, pp. 131–141, 2017, doi:10.1007/s12651-017-0225-5.

[4] R. Peled, Y. & Sharon, "Gender Effect on Student Teachers' Attitudes toward Peer Feedback in a Wiki Learning Environment," *Proceedings of SITE 2015--Society for Information Technology & Teacher Education International Conference*, vol. 3, no. 2, pp. 693–700, 2015.

[5] J. Archer, S. Freedman, "Gender-Stereotypic Perceptions of Academic Disciplines," *British Journal of Educational Psychology*, vol. 59, no. 3, pp. 306–313, 1989, doi:10.1111/j.2044-8279.1989.tb03105.x.

[6] A. M. Koenig et al., "Are leader stereotypes masculine? A meta-analysis of three research paradigms.," *Psychological Bulletin*, vol. 137, no. 4, pp. 616–642, 2011, doi:10.1037/a0023557.

[7] Z. Merchant et al., "Effectiveness of virtual reality-based instruction on students' learning outcomes in K-12 and higher education: A meta-analysis," *Computers & Education*, vol. 70, no. hal 140, pp. 29–40, 2014, doi:10.1016/j.compedu.2013.07.033.

[8] Younis Illahi Bhat, "Academic Achievements and Study Habits of College Students of District Pulwama," *Journal of Education and Practice*, vol. 7, no. 10, pp. 2016, 2016.

[9] E. Stork, N. T. Hartley, "Classroom Incivilities: Students Perceptions About Professors Behaviors," *Contemporary Issues in Education Research (CIER)*, vol. 2, no. 4, pp. 13, 2011, doi:10.19030/cier.v2i4.1066.

[10] S. N. O. Abdul Qawi Noori, "The Challenges of Undergraduate Married Female Students in Higher Education: A case study of Takhar University," *Journal of World Englishes and Educational Practices (JWEEP)*, vol. 3, no. 6, pp. 15, 2021, doi:10.32996/jweep.

[11] D. G/Tsadik et al., "Theoretical bases of social-emotional learning intervention programs for preschool children," *International Online Journal of Education and Teaching (IOJET)*, vol. 7, no. 4, pp. 1517–1531, 2020.

[12] H. S. Akareem, S. S. Hossain, "Perception of education quality in private universities of Bangladesh: A study from students' perspective," *Journal of Marketing for Higher Education*, vol. 22, no. 1, pp. 11–33, 2012, doi:10.1080/08841241.2012.705792.

[13] N. Y. Hwang, B. Fitzpatrick, "Student–Teacher Gender Matching and Academic Achievement," *AERA Open*, vol. 7, no. 1, pp. 2021, 2021, doi:10.1177/23328584211040058.

[14] K. Kwok, J. Potter, "Gender stereotyping in student perceptions of teaching excellence: applying the shifting standards theory," *Higher Education Research and Development*, pp. 7294360, 2021, doi:10.1080/07294360.2021.2014411.

[15] A. Arrona-Palacios et al., "Does professors' gender impact how students evaluate their teaching and the recommendations for the best professor?," *Heliyon*, vol. 6, no. 10, pp. e05313, 2020, doi:10.1016/j.heliyon.2020.e05313.

[16] S. O. Appiah, "Impact of Lecturers' Gender on Learning: Assessing University of Ghana Students' Views," vol. 2, no. 10, pp. 44–68, 2018.

[17] S. Rajesh Shah, U. S. Udgaonkar, "Influence of Gender and Age of Teachers on Teaching: Students Perspective," *International Journal of Current Microbiology and Applied Sciences*, vol. 7, no. 1, pp. 2436–2441, 2018, doi:10.20546/ijcmas.2018.701.293.

[18] N. Ambady et al., "Stereotype Susceptibility in Children: Effects of Identity Activation on Quantitative Performance," *Psychological Science*, vol. 12, no. 5, pp. 385–390, 2001, doi:10.1111/1467-9280.00371.

GORDON AMIDU has done his Diploma in Librarianship and bachelor's degree in Information Studies from the University of Ghana in 2011 and 2015.He has a master's degree in library and information science earning a first-class with distinction from Andhra University in 2022. His areas of interest are information behavior, international information issues, gender and information technology, electronic resources and digital libraries.

Received: 02 May 2022, Revised: 30 June 2022, Accepted: 01 July 2022, Online: 18 July 2022

DOI: https://dx.doi.org/10.55708/js0107004

Acceleration of Image Processing with SHA-3 (Keccak) Algorithm using FPGA

Argyrios Sideris*, Theodora Sanida, Dimitris Tsiktsiris, Minas Dasygenis

Department of Electrical & Computer Engineering, University of Western Macedonia, Kozani, 50131, Greece

*Corresponding author: , Argyrios Sideris, UOWM Kozani, asideris@uowm.gr

ABSTRACT: In our digital world, the transmission of images between people has played an essential part in everyday communication. As a result, procedures to ensure the integrity and accuracy of the communicated data are required. Today, hashing is the most popular and secure way. This article focuses on the SHA-3 for hashing images dimensions 256×256 pixels with our custom implementations on the FPGA based on the Very High Speed Integrated Circuit Hardware Description Language (VHDL). We perform our experiments on the Intel Arria 10 GX FPGA and the Nios II processor. Also, our experiments with calculating metrics such as entropy, NPCR and UACI show that the SHA-3 is secure, reliable and has high application potential for hashing images. We propose designs to improve throughput, security, and efficiency criteria. We strengthened our design using the IP Block Floating Point Hardware 2 (FPH-2). Our experiments with the proposed implementation have shown increased throughput by 14.38% and efficiency by 13.95% of the SHA-3 algorithm. Finally, we compared our findings to other researchers' existing optimization methodologies, giving data that demonstrate our research's strengths.

KEYWORDS Pipeline, Cryptography, SHA-3, Keccak hash function, FPGA, NIOS II Processor, Floating point hardware

1. Introduction

As well as for any other transmitted information, the integrity of the image transfer is achieved via cryptographic hashing functions. An essential role in today's world of digital transmissions plays cryptographic hash functions. It is an essential technology used to protect information integrity when information is transmitted over a grid. Nowadays, image information security is crucial, mainly in the army, meteorology, medicine, intelligent robots, commerce, etc. As a result, the cryptographic society's mission has become the creation of an image hash feature [1]–[3].

Watermarking is the technique for guarding digital images and video against alterations or corruption. Hash features can be successfully used in range authentication and image watermark applications [4]. In expansion, a picture hash procedure would significantly simplify investigations. Moreover, hashing is utilized within comparisons in vast databases, in which a lot of similar arrangements of an image can exist [5].

In this paper, we developed and implemented the famous Keccak (SHA3-256) algorithm in the Intel Arria 10 GX FPGA board. We utilised the new algorithm SHA-3 with a 256-bits output size because it provides high safety and maintains the original image quality during the hash process. We provide a FPH-2-based approach in our tailor-made design. We compare the two strategies we have designed with other similar models and with standard evaluation criteria (entropy, Unified Averaged Changed Intensity (UACI), Number of Pixel Changing Rate (NPCR), efficiency and throughput).

The main contributions of our work are:

- We suggest a novel two-stage pipelined design for the SHA-3 algorithm in 256 bits output length for 256×256 pixel images, optimizing FPGA devices' acceleration and performance. We have used SHA-3 with a 256-bits output length because it provides high security.

- We contribute an innovative procedure established on the FPH-2 element in our design, which delivers an inferior cycle count. We analysed the optimisation plan to maximise the throughput and efficiency measures, and at the same time, algorithm SHA-3 keeps the actual image quality.

The remains of the article are organized as follows: In the next Section 2, we introduce study works which are similar to ours. In Section 3, we outline our experiments in detail for the implementation of SHA3-256 (Keccak) in 256×256 pixel images on an Intel Arria 10 GX FPGA device. In Section 4, we show and discuss the testing results and the implementation evaluation of our work. Finally, in Section 5, we outline our study's conclusions and future work.

2. Related work

From the literature review, we selected similar works for comparison. We chose the specific articles because they are up to date state of the art designs using the SHA-3 algorithm. The objective of all these models is to enhance performance while at the same period trying to decrease power consumption and area on the FPGA board.

An efficient and secured image encryption algorithm is proposed in [6], jointly using the SHA-3 hash function with two-dimensional Arnold chaotic maps. In the permutation step, a conventional encryption technique is described with four random shuffling rules to avoid time consumption in the pixel position index sorting phase. Numerical findings reveal that the proposed encryption technique may improve security and speed up the implementation of digital picture transmission.

On work [7], the authors focus on 256 × 256 grayscale image encryption. The implementation was done using VHDL. The results show that the proposed architecture for the SHA3-256 algorithm achieved a throughput of 35.593 Gbps, maximum frequency of 458 MHz, area (slices) 2.984 and efficiency of 11.92 Mbps/Slices.

The authors in [8] suggest a new implementation with a chaotic encryption algorithm for images in dual chaotic maps. The SHA-3 and an auto updating system calculate the hash values to construct a Logistic map's control parameter and initial condition. Behind that, all the permutations are executed for rows and columns in an image to exchange pixels. As an effect, the presented algorithm can oppose known-plaintext attacks efficiently.

On work [9], the authors focus on all candidates in the SHA-3 competition in terms of their effectiveness in the area (slices). Their research was conducted with the Virtex-5 and Virtex-6 FPGA devices. The implementation was done using VHDL. Their architecture for the SHA3-256 algorithm achieved better results with the Virtex-6 device with a throughput of 1.071 Gbps, maximum frequency of 197 MHz, area (slices) 397 and efficiency of 2.69 Mbps/Slices.

The authors in [10] focus on all candidates in the SHA-3 finalists in the FPGA. The main goal of the research is to analyze the performance of all candidates in terms of throughput and area. In their work, they used a Virtex 5 and Virtex 6 from Xilinx and Stratix III and Stratix IV from Intel and the implementation was done using VHDL. The results show that the proposed architecture for the SHA3-256 (Keccak) algorithm achieves better results with the Virtex-6 device. They achieved a throughput of 16.236 Gbps, area (slices) 1.446 and efficiency of 11.23 Mbps/Slices.

In [11], the authors work on the assessment of all SHA-3 finalists in FPGA devices. The primary goal of their work is to compare all candidates with the evaluation criteria of throughput, clock frequency and area. Their research was conducted with Virtex-5, 6 and 7 FPGA devices. The implementation was done using VHDL. The results show that the proposed design for the SHA-3 algorithm achieves better results with the Virtex-5 device in clock frequency, region and performance than other candidates.

The authors in [12] deal with the performance implementation of all SHA-3 finalists in the FPGA. The main goal of the research is to provide a fair and comprehensive evaluation of all candidates in terms of throughput and area. Their work used a Xilinx Virtex-5 and Virtex-6 device, and the implementation was done using VHDL. Their architecture for the SHA3-256 (Keccak) algorithm with the Virtex-6 device achieved a throughput of 12.817 Gbps and efficiency of 10.08 Mbps/Slices, a maximum frequency of 282.7 MHz and an area (slices) of 1.272.

In [13], the authors investigated the calculatedly efficiency of all SHA-3 finalists in FPGA devices. The primary purpose of this study is to compare the efficacy of this design in terms of fragmented functions per unit area. The work was done using a Virtex-5 FPGA chip with VHDL as the implementation language. The suggested design for the SHA3-256 (Keccak) algorithm requires 1.117 slices (area), reaches a maximum frequency of 189 MHz, and has a throughput of 6.263 Gbps and an efficiency of 3.17 Mbps/Slices, according to the results.

The authors in [14] deal with the effective implementation of all SHA-3 finalists in the FPGA. The main goal of the research is to provide a basic comparison between all candidates in terms of clock frequency, throughput and area. They used a Xilinx FPGA device in their work, and the implementation was done using VHDL. Their architecture for the SHA3-256 algorithm achieved a throughput of 11.9 Gbps, a maximum frequency of 215 MHz, and an area (slices) of 4.745.

On work [15], the authors suggested a pipelining architecture for the SHA-3 algorithm in order to raise its efficiency and throughput of them. The proposed architectures were implemented in FPGA Virtex-2, Spartan-3 and Virtex-4 using Verilog. According to the experimental findings, the suggested designs provide excellent performance with the Virtex-4 device in terms of total area, maximum frequency, throughput, and throughput/area.

All of these documents and many more [16]–[25], have as their main goal the increase of its throughput and efficiency metrics in the SHA3 (Keccak) algorithm. However, improved architecture is always needed to enhance throughput and efficiency. Compared to previous works, we designed and implemented two designs of the SHA3, using the Nios II/f processor. Our first design applies a two-stage pipeline architecture. The second concerns a method based on the FPH-2 part in a two-stage pipeline design. The two approaches we suggest in this paper deliver a secure SHA3 with 256bits hashing implementation. The proposed design with the FPH-2 component and the two-stage pipelined architecture outperforms existing implementations.

3. Implementation for Image Hashing

This section analyses all the design components we have implemented for the SHA3-256 (Keccak). In our experiments, we have used the Standard Edition (SE) Quartus II ver. 18.3 and the DE5a-Net board. Table 1 displays the specifications of the Terasic DE5a-Net board.

3.1. Nios II - Soft-Core Embedded Processor

The Nios II is wholly implemented in the FPGA. It is considered suitable for most embedded applications and provides flexibility for real-time and cost-sensitive functionality [26]. Nios II is offered in three different configurations: fast, standard and economy. The Nios fast is optimized for the most high performance; this performance can be modified using patronage instructions, hardware accelerators, and the highest bandwidth switch fabric. The Nios standard is used for increased performance, and Nios economy is appropriate for mediocre performance [27].

Table 1: FPGA Specifications

Parameters	Values
FPGA id	10AX115N2F45E1SG
Board	Terasic Intel Arria® 10 GX FPGA
System Clock Frequency	50MHz Oscillator
Memory	SO-DIMM 2400 MHz SDRAM 2x4GB DDR4

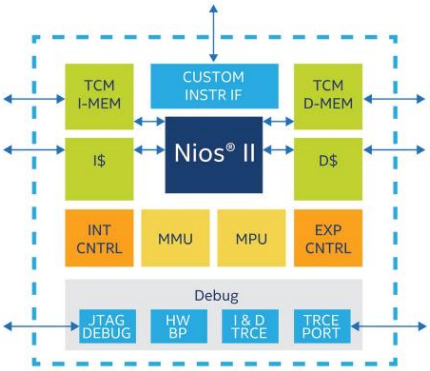


Figure 1: Nios® II processor family Fast (/f core): Six-stage pipeline optimized for highest performance, optional memory management unit (MMU), or memory protection unit (MPU) [27].

In our experimentations, we utilised the processor NIOS II/f, as shown in Figure 1. Its main characteristics are operation with a 6-stage pipeline to gain the external interrupt controller, custom instructions, highest DMIPS/MHz and optional hardware multiply to improve arithmetic performance [28, 29].

3.2. Nios II Custom Instruction Implementation

Custom instructions provide us with the capability to feet the Nios II processor to complete the requirements of an application. A custom instruction logic block interfaces with the Nios II processor through 3 ports: $data_a$, $data_b$, and result. The custom instruction obtains input on its $data_a$ port and $data_b$ ports and drives the final results to its result port. A conduit interface to external logic provides a custom interface to method resources exceeding the Nios II processor. A custom combination statement complements its logical function in a single clock cycle. Custom multi-cycle instructions require two or more time cycles to operate. An extended custom instruction allows the implementation of several different operations. An Internal register file allows to access the Nios II for input or output or both [30].

Figure 2 shows a block graph with all ports of a Nios II custom instruction.

3.3. Floating Point Hardware 2 (FPH-2)

We may choose to avoid the floating-point divider because it takes more resources than other instructions. If Nios II does not employ floating-point division, we may choose to do so. We can rearrange our code in some cases to reduce or even eliminate separated processes.

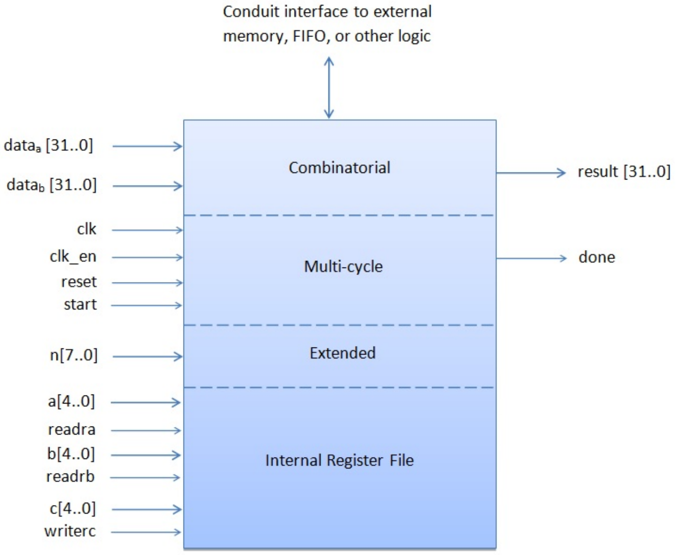


Figure 2: Custom Instruction types with all ports of the Nios II processor.

Table 2: FPH-2 operations implemented

Floating Point Hardware 2 custom instruction	
Multi-Cycle Custom Instruction	Combinatorial Custom Instruction
add multiply subtract divide square root convert	minimum maximum absolute compare negate

Minimum, maximum, negate, absolute, and comparisons are all provided via the special instruction implementations. FPH-2 is preferred over FPH-1 legacy because it has a lower clock cycle count, better acceleration, and a smaller area. In addition, the FPH-2 component helps with FPH-1 procedures and rounding accuracy, which is not an IEEE 754-defined rounding mode [30]. The floating functions performed by each custom orders are listed in Table 2.

3.4. System Design of the SHA3-256 Core

FPH-2 is supported by the Nios II architecture. Low cycle count implementations are possible with the FPH-2 component. Addition, subtraction, square root integer to float conversion, multiplication, float to integer conversion, and division are the most common floating point custom instructions. The SHA3-256 proposed system is depicted in Figure 3. The Xor Input bitrate, Zero State, Control Unit, Counter and Keccak Round are built into the structure. The initial zero status is retained in the zero status component of the first iteration of SHA-3.

While compile a multi-block message, the multiplexer is used to provide feedback. The Xor Input bitrate element combines the XOR bits of the bitrate state matrix with the bits of the Input block, which are the result of the infill procedure. The control, coordination and communication of the data flow within the design is the responsibility of the control unit. The Control Unit signal enables the meter. The Keccak RC is described in the following subsection.

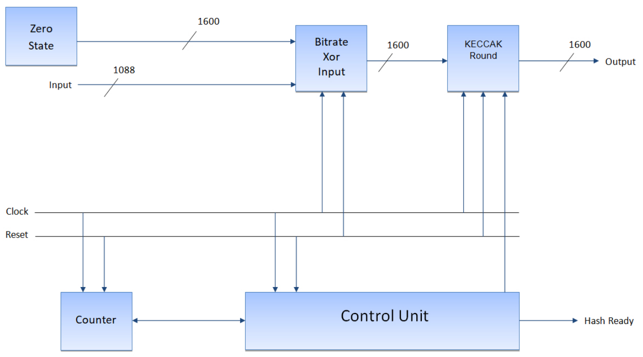


Figure 3: The design of the whole system for the SHA3-256 Core.

3.5. The SHA-3 Pipelined Design

The SHA-3 has 24 modification phases, each of which is made up of five phases: $\boldsymbol{\theta}, \boldsymbol{\rho}, \boldsymbol{\pi}, \boldsymbol{\chi}$ and $\boldsymbol{\iota}$, signified as theta, rho, pi, chi, and iota respectively. SHA-3 (Keccak) takes the state array per step and produces a newly updated state array after using the related state function. Figure 4 shows the Keccak Round's two-staged pipelined design.

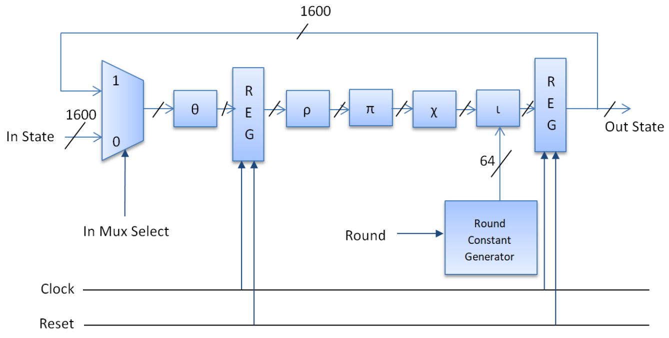


Figure 4: Two-staged pipelined design of the Keccak Round.

There is a 2-in-1 multiplexer for the round's feedback at the start of the round. In each round, we use the pipelined approach to enter two registers. Between portions, the first register is located $\boldsymbol{\theta}$ and $\boldsymbol{\rho}$ in order to separate the crucial path by nearly half. The second register is located just before the feedback unit at the end of the round. The clock and reset are the control signals of the two registers. The RC is put in the $\boldsymbol{\iota}$ procedure produced by the RC generator and is shown in Table 3.

3.6. System Integration

The original grayscale image had a resolution of 256×256 pixels. The SDRAM memory stores the input block. The block is then fed into the SHA-3 core as input. The SHA-3 core's output block is saved in SDRAM memory. VHDL was used to implement all of the components. Using a variety of test benches, we inspected each VHDL file to ensure its validity and usefulness. The ModelSim 10.6d simulator was used to run all of the tests on each VHDL file, with valid input data sheets given by NIST for the SHA-3 algorithm in [31].

In addition, we used ModelSim 10.6d to simulate the top module using legitimate input examples for the SHA-3 algorithm provided by NIST in [32]. We moved on to the design of the Nios II CPU after correctly verifying the simulation outcomes in ModelSim 10.6d.

Table 3: The RC Generator RC_i in Iota function

RC_0	0x0000000000000001	RC_{12}	0x000000008000808B
RC_1	0x0000000000008082	RC_{13}	0x800000000000008B
RC_2	0x800000000000808A	RC_{14}	0x8000000000008089
RC_3	0x8000000080008000	RC_{15}	0x8000000000008003
RC_4	0x000000000000808B	RC_{16}	0x8000000000008002
RC_5	0x0000000080000001	RC_{17}	0x8000000000000080
RC_6	0x8000000080008081	RC_{18}	0x000000000000800A
RC_7	0x8000000000008009	RC_{19}	0x800000008000000A
RC_8	0x000000000000008A	RC_{20}	0x8000000080008081
RC_9	0x0000000000000088	RC_{21}	0x8000000000008080
RC_{10}	0x0000000080008009	RC_{22}	0x0000000080000001
RC_{11}	0x000000008000000A	RC_{23}	0x8000000080008008

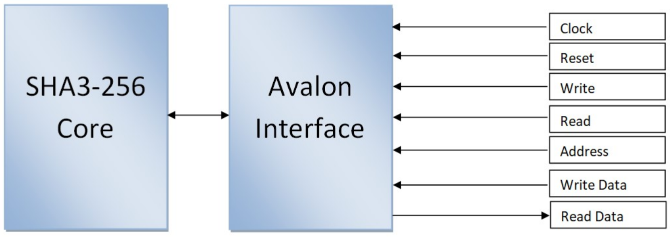


Figure 5: Avalon Switch Fabric and SHA3-256 Core data transfer.

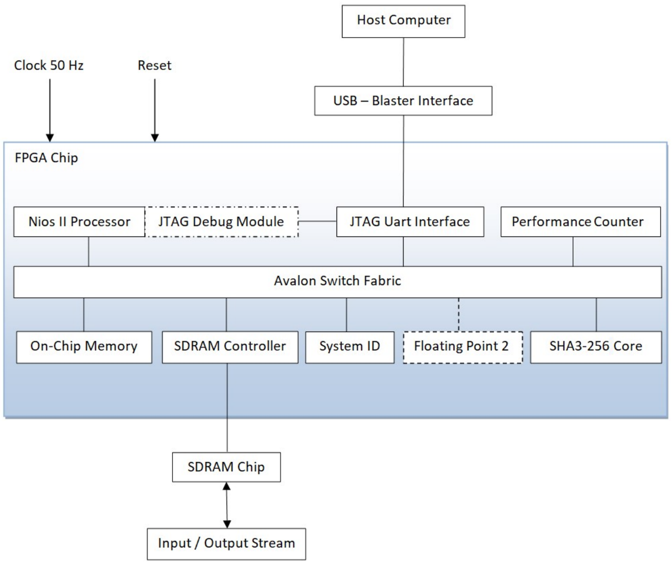


Figure 6: The whole chart of the system on the FPGA.

The designer platform was used to create the Nios II processor's scheme. We utilised the Nios II fast soft-core, which has a high-performance speed and maximises the processor core's f_{MAX} performance. Clock, On-chip RAM, controller of SDRAM, a counter of performance, PLL, Peripheral ID System, JTAG-UART, and custom component SHA-3-256 are among the Nios II system's implemented components. The operating memory for the Nios II CPU is on-chip RAM. As demonstrated in Figure 5, all information is sent from Nios II to the SHA-3 feature via the Avalon Switch Fabric.

Figure 6 displays the whole structure of our architecture that we built using the Nios II soft-core.

4. Experimental Results

The test were carried out using the Arria 10 GX FPGA. We designed a novel two-staged pipelined design with the FPH-2 component and a two-staged pipelined design.

4.1. Image and Histogram Analysis

Figure 7 (b) shows the histogram of the classical images ("Lena", "Camera man" and "Pepper") in Figure 7 (a). In the histogram, the horizontal axis denotes the gray level, and the vertical axis denotes the pixel number of each gray level. After being encrypted by the SHA3-256 (Keccak) algorithm, the histogram of the cipher-image is completely uniform and absolutely different from that of the plain-image as shown in Figure 7 (d).

4.2. Entropy Analysis

The entropy of a photograph is a statistical metric for determining how random a coded image is. It also describes the median information of an image origin. The entropy $E(X)$ is calculated in (1), where X represents the test photo, x_{i} symbolizes the cost in X, and $Pr(x_{\mathrm{i}})$ indicates the chance of $X = x_{\mathrm{i}}$.

$$E(X) = \sum_{i=1}^{n} \Pr(x_i) \log_2 \Pr(x_i) \tag{1}$$

Table 4: The entropies of fragmented images and comparison

Images	This Work	Ref.[6]	Ref.[7]	Ref.[8]
Boat	7.9994	7.991	7.9993	7.991
Lena	7.9990	7.990	7.9989	-
Cameraman	7.9992	-	7.9991	-
Peppers	7.9995	-	7.9994	7.991
Baboon	7.9996	7.992	7.9995	7.992

The entropy of a large number of hashed photos was calculated. The results are presented in Table 4, which shows that the hashed image entropy's are extremely near to 8. For a 256 gray-scale photo, the max entropy is $log_2(256) = 8$. As a result, the suggested picture hashing approach has a high resistance against entropy attacks.

4.3. Correlation Analysis

Pixels should have a strong neighborhood correlation, which is one of the most important properties of an image. For the design to be considered secure and effective, there must be no correlation between pixels in an encrypted image. The correlation coefficient is given by in (2), where x_{i} and y_{i} is a pair of neighboring pixels that are horizontally, vertically, and diagonally adjacent, M signifies the total number of neighboring pixel pairs.

$$r_{xy} = \frac{\sum_{i=1}^{M}\left(x_i - \frac{1}{M}\sum_{j=1}^{M} x_j\right)\left(y_i - \frac{1}{M}\sum_{j=1}^{M} y_j\right)}{\sqrt{\sum_{i=1}^{M}\left(x_i - \frac{1}{M}\sum_{j=1}^{M} x_j\right)^2}\sqrt{\sum_{i=1}^{M}\left(y_i - \frac{1}{M}\sum_{j=1}^{M} y_j\right)^2}} \tag{2}$$

Table 5 shows the correlation coefficients in the three orientations, demonstrating that the encrypted image correlation coefficients are very close to 0. As a result, the suggested model is resistant to statistical attacks.

Table 5: Correlations coefficients of encrypted images

Image	Direction	Correlation
Lena	Horizontal	0.001214
	Vertical	0.006210
	Diagonal	0.003216
Camera man	Horizontal	0.001368
	Vertical	0.007410
	Diagonal	0.004126
Peppers	Horizontal	0.001424
	Vertical	0.007128
	Diagonal	0.005210

4.4. NPCR and UACI Metrics Analysis

We use the Number of Pixel Change Rates (NPCR) and Unified Average Changing Intensity (UACI) to calculate the result of switching one pixel in both plain and hashed photos. [33]. The NPCR measures the number of individual pixels between the two images, and the UACI measures the average intensity. The NPCR is computed using (3), where D represents the bipolarity array with comparable size as the prototype image and hashes image, $M \times N$ define the size of the picture.

$$\mathrm{NPCR} = \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} \mathrm{D(i,j)} \times \frac{100\%}{\mathrm{M} \times \mathrm{N}} \tag{3}$$

The UACI calculated using (4), where C_1 denotes the original image, C_2 is the hashed picture and $M \times N$ define the size of the picture in pixels.

$$\mathrm{UACI} = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times \frac{100\%}{M \times N} \tag{4}$$

The findings of the NPCR and the UACI are shown in Table 6. The high values of the NPCR and UACI measurements imply that hashing is more secure and more resistant to differential assaults.

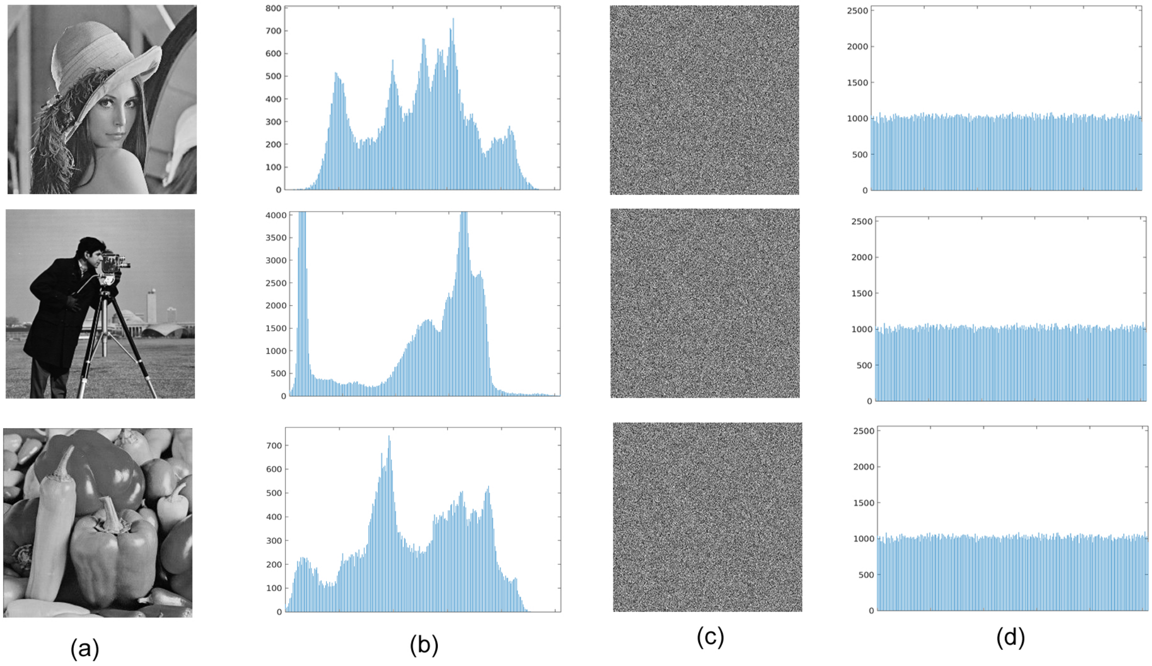


Figure 7: (a) plain-image, (b) histogram of the plain-image, (c) cipher-image and (d) histogram of the cipher-image.

Table 6: The NPCR and the UACI results and comparison

Images	This Work		Ref. [6]		Ref. [7]		Ref. [8]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Boat	99.644	33.652	99.629	33.529	99.6420	33.6463	-	-
Lena	99.692	33.688	99.554	33.392	99.6886	33.6818	99.603	33.432
Cameraman	99.660	33.662	99.598	33.534	99.6543	33.6592	99.641	33.498
Peppers	99.634	33.640	-	-	99.6321	33.6326	-	-
Baboon	99.662	33.664	99.615	33.402	99.6563	33.6531	99.600	33.428

4.5. Throughput and Efficiency Metrics

The throughput (TH) is computed using (5). In the (5), *Number of bits* is the bitrate size r, *frequency* is the maximum frequency reported by the tool and *Number of clock cycles* denote the latency of the circuit. Clock cycles represent the number of resumption needed of the five functions $\boldsymbol{\theta}$, $\boldsymbol{\rho}$, $\boldsymbol{\pi}$, $\boldsymbol{\chi}$ and $\boldsymbol{\iota}$ to generate the hash value.

$$TH = \frac{Number\ of\ bits \times frequency}{Number\ of\ clock\ cycles} \tag{5}$$

The efficiency (EF) is computed by using (6).

$$EF = \frac{TH}{Area} \tag{6}$$

The findings of our two designs for the SHA3-256 (Keccak) algorithm are shown in Table 7. The number of clock cycles of the five functions in a two-staged pipelined design is 18, while the number of clock cycles in a two-staged pipelined design with the component FPH-2 is 14.

Since the number of clock cycles is reduced and the maximum clock frequency increases, the proposed design of a two-staged pipelined architecture with FPH-2 provides the highest efficiency and throughput.

Table 7: The results for Efficiency and Throughput of our two designs

Design	**Area (Slices)**	**Frequency (MHz)**	**Throughput (Gbps) (r = 1088)**	**Efficiency (Mbps/Slices) (r = 1088)**
Proposed architecture with two-staged pipeline	2682	432	25.507	9.51
Proposed architecture with two-staged pipeline and FPH-2	2764	472	36.681	13.27

Table 8 presents the comparison with other similar architectures, taking into account their best implementation in terms of the criteria of throughput and efficiency for the SHA3-256 (Keccak) algorithm. When using the component FPH-2 to implement the proposed design, the area was raised by 10.30% (slices), but the maximum clock improved by 10.92% (frequency) and increased by 12.85% the number of clock cycles, resulting in a 14.38% increase in throughput and a 13.95% increase inefficiency.

Researchers in the works [9, 11, 12, 13, 20, 21, 22] show a smaller area compared to our implementations, but the frequency they achieve is lower than our experimental applications. Also, in the work [15] there is a higher frequency than the one we achieved, but they show a large increase in the area. Finally, in the works [7, 14, 18] the researchers

Table 8: Throughput - Efficiency results and comparison for the SHA-3 algorithm

Work	FPGA Device	Frequency (MHz)	Area (Slices)	Throughput (Gbps) (r = 1088)	Efficiency (Mbps/Slices) (r = 1088)
Kitsos P. *et al.* (2010) [14]	-	215	4745	11.9	2.50
Akin A. *et al.* (2010) [15]	Virtex-4	509	4356	22.33	5.13
Kaps J. P. *et al.* (2012) [21]	Virtex-6	299	106	0.136	1.28
Provelengios G. *et al.* (2012) [20]	Virtex-5	285	2573	5.70	2.21
Gaj K. *et al.* (2010) [12]	Virtex-6	282.7	1272	12.817	10.08
Jararweh Y. *et al.* (2012) [11]	Virtex-5	271	1414	12.28	8.68
Sideris A.*et al.* (2022) [7]	Arria 10 GX	458	2984	35.593	11.92
Gholipour A. *et al.* (2012) [18]	Altera Stratix III	212.49	5633	13.59	2.41
Baldwin B. *et al.* (2010) [13]	Virtex-5	189	1117	6.263	3.17
Kobayashi K. *et al.* (2010) [22]	Virtex-5	205	1433	8.40	5.86
Homsirikamol E. *et al.* (2011) [10]	Virtex-6	-	1446	16.236	11.23
Jungk B. (2011) [9]	Virtex-6	197	397	1.071	2.69
Proposed design with FPH-2	**Arria 10 GX**	**472**	**2764**	**36.681**	**13.27**

show a larger area and smaller frequency than we achieved with our architectures. In our architectures, the primary purpose was not to use an excessive growth of the cost of the area (Slices) so that the throughput (Gbps) and efficiency (Mbps/Slices) are not burdened.

5. Conclusions and Future Work

The optimal performance of hashing images with a size of 256×256 pixels using the SHA-3 algorithm with the Nios II/f (fast) soft-core processor in the FPGA Intel Arria 10 GX is presented in this study.

We choose the SHA-3 algorithm, which has a 256-bit output length, because it provides the best security and performance. Our testing using the proposed two-staged pipelined design and the bespoke FPH-2 component revealed that the SHA-3 algorithm had a 14.38% percent improvement in throughput and a 13.95% percent gain inefficiency. At the same time, we increased the minimum area by 10.30% (slices), the max clock signal by 10.92% (frequency), and by 12.85% the number of clock cycles. The suggested approach combines speed, performance, and security to produce the optimum solution for hashing images with a dimension of 256×256 pixels.

In the future, we'll experiment with picture hashing using Tree Hashing and a simpler design with fewer rounds (12 instead of the 24 in SHA-3).

Conflict of Interest The authors declare no conflict of interest.

References

[1] S. Agarwal, "Secure image transmission using fractal and 2d-chaotic map", *Journal of Imaging*, vol. 4, no. 1, p. 17, 2018, doi: 10.3390/jimaging4010017.

[2] A. Girdhar, H. Kapur, V. Kumar, "A novel grayscale image encryption approach based on chaotic maps and image blocks", *Applied Physics B*, vol. 127, no. 3, pp. 1–12, 2021, doi:10.1007/s00340-021-07585-x.

[3] X. Kang, R. Tao, "Color image encryption using pixel scrambling operator and reality-preserving mpfrht", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 7, pp. 1919–1932, 2018, doi:10.1109/TCSVT.2018.2859253.

[4] A. Swaminathan, Y. Mao, M. Wu, "Robust and secure image hashing", *IEEE Transactions on Information Forensics and security*, vol. 1, no. 2, pp. 215–230, 2006, doi:10.1109/TIFS.2006.873601.

[5] V. Monga, A. Banerjee, B. L. Evans, "A clustering based approach to perceptual image hashing", *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 68–79, 2006, doi:10.1109/TIFS.2005.863502.

[6] G. Ye, H. Zhao, H. Chai, "Chaotic image encryption algorithm using wave-line permutation and block diffusion", *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2067–2077, 2016, doi:10.1007/s11071-015-2465-7.

[7] A. Sideris, T. Sanida, D. Tsiktsiris, M. Dasygenis, "Image hashing based on sha-3 implemented on fpga", "Recent Advances in Manufacturing Modelling and Optimization", pp. 521–530, Springer, 2022, doi:10.1007/978-981-16-9952-8_44.

[8] G. Ye, X. Huang, "A secure image encryption algorithm based on chaotic maps and SHA-3", *Security and Communication Networks*, vol. 9, no. 13, pp. 2015–2023, 2016, doi:10.1002/sec.1458.

[9] B. Jungk, J. Apfelbeck, "Area-efficient fpga implementations of the sha-3 finalists", "2011 International Conference on Reconfigurable Computing and FPGAs", pp. 235–241, IEEE, 2011, doi: 10.1109/ReConFig.2011.16.

[10] E. Homsirikamol, M. Rogawski, K. Gaj, "Comparing hardware performance of round 3 sha-3 candidates using multiple hardware architectures in xilinx and altera fpgas", "Ecrypt II Hash Workshop", vol. 2011, pp. 1–15, 2011, doi:10.1001/ICT-2007-216676.

[11] Y. Jararweh, H. Tawalbeh, A. Moh'd, *et al.*, "Hardware performance evaluation of sha-3 candidate algorithms", *Journal of Information Security*, 2012, doi:10.4236/jis.2012.32008.

[12] K. Gaj, E. Homsirikamol, M. Rogawski, "Fair and comprehensive methodology for comparing hardware performance of fourteen round two sha-3 candidates using fpgas", "International Workshop on Cryptographic Hardware and Embedded Systems", pp. 264–278, Springer, 2010, doi:10.1007/978-3-642-15031-9_18.

[13] B. Baldwin, A. Byrne, L. Lu, M. Hamilton, N. Hanley, M. O'Neill, W. P. Marnane, "Fpga implementations of the round two sha-3 candidates", "2010 International Conference on Field Programmable Logic and Applications", pp. 400–407, IEEE, 2010, doi:10.1109/FPL.2010.84.

[14] P. Kitsos, N. Sklavos, “On the hardware implementation efficiency of sha-3 candidates”, “2010 17th IEEE International Conference on Electronics, Circuits and Systems”, pp. 1240–1243, IEEE, 2010, doi: 10.1109/ICECS.2010.5724743.

[15] A. Akin, A. Aysu, O. C. Ulusel, E. Savaş, “Efficient hardware implementations of high throughput sha-3 candidates keccak, luffa and blue midnight wish for single-and multi-message hashing”, “Proceedings of the 3rd International Conference on Security of Information and Networks”, pp. 168–177, 2010, doi:10.1145/1854099.1854135.

[16] I. San, N. At, “Compact keccak hardware architecture for data integrity and authentication on fpgas”, *Information Security Journal: A Global Perspective*, vol. 21, no. 5, pp. 231–242, 2012, doi: 10.1080/19393555.2012.660678.

[17] A. Sideris, T. Sanida, M. Dasygenis, “High throughput pipelined implementation of the sha-3 cryptoprocessor”, “2020 32nd International Conference on Microelectronics (ICM)”, pp. 1–4, IEEE, 2020, doi:10.1109/ICM50269.2020.9331803.

[18] A. Gholipour, S. Mirzakuchaki, “High-speed implementation of the keccak hash function on fpga”, *International Journal of Advanced Computer Science*, vol. 2, no. 8, pp. 303–307, 2012, doi: 10.1142/S0218126616500262.

[19] A. Sideris, T. Sanida, M. Dasygenis, “High throughput implementation of the keccak hash function using the nios-ii processor”, *Technologies*, vol. 8, no. 1, p. 15, 2020, doi:10.3390/technologies8010015.

[20] G. Provelengios, P. Kitsos, N. Sklavos, C. Koulamas, “Fpga-based design approaches of keccak hash function”, “2012 15th Euromicro Conference on Digital System Design”, pp. 648–653, IEEE, 2012, doi:10.1109/DSD.2012.63.

[21] J.-P. Kaps, P. Yalla, K. K. Surapathi, B. Habib, S. Vadlamudi, S. Gurung, “Lightweight implementations of sha-3 finalists on fpgas”, “The Third SHA-3 Candidate Conference”, pp. 1–17, 2012, doi: 10.1007/978-3-642-25578-6_20.

[22] K. Kobayashi, J. Ikegami, M. Knežević, E. X. Guo, S. Matsuo, S. Huang, L. Nazhandali, Ü. Kocabaş, J. Fan, A. Satoh, *et al.*, “Prototyping platform for performance evaluation of sha-3 candidates”, “2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)”, pp. 60–63, IEEE, 2010, doi:10.1109/HST.2010.5513111.

[23] F. Kahri, H. Mestiri, B. Bouallegue, M. Machhout, “High speed fpga implementation of cryptographic keccak hash function crypto-processor”, *Journal of Circuits, Systems and Computers*, vol. 25, no. 04, p. 1650026, 2016, doi:10.1142/S0218126616500262.

[24] G. S. Athanasiou, G.-P. Makkas, G. Theodoridis, “High throughput pipelined fpga implementation of the new sha-3 cryptographic hash algorithm”, “2014 6th International Symposium on Communications, Control and Signal Processing (ISCCSP)”, pp. 538–541, IEEE, 2014, doi:10.1109/ISCCSP.2014.6877931.

[25] L. Ioannou, H. E. Michail, A. G. Voyiatzis, “High performance pipelined fpga implementation of the sha-3 hash algorithm”, “2015 4th Mediterranean Conference on Embedded Computing (MECO)”, pp. 68–71, IEEE, 2015, doi:10.1109/MECO.2015.7181868.

[26] Intel®FPGA, “Classic processor reference guide”, *online* *https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/hb/nios2/n2cpu_nii5v1.pdf*, (accessed on 12 December 2021).

[27] Intel®FPGA, “Nios® II processors for fpgas”, *online* *https://www.intel.com/content/www/us/en/products/programmable/processor/nios-ii.html*, (accessed on 15 December 2021).

[28] A. Sideris, T. Sanida, M. Dasygenis, “Hardware acceleration of sha-256 algorithm using nios-ii processor”, “2019 8th International Conference on Modern Circuits and Systems Technologies (MOCAST)”, pp. 1–4, IEEE, 2019, doi:10.1109/MOCAST.2019.8741638.

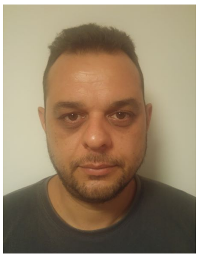
[29] A. Sideris, T. Sanida, M. Dasygenis, “Hardware acceleration of the aes algorithm using nios-ii processor”, “2019 Panhellenic Conference on Electronics & Telecommunications (PACET)”, pp. 1–5, IEEE, 2019, doi:10.1109/PACET48583.2019.8956285.

[30] Intel®FPGA, “Nios II custom instruction user guide”, *online* *https://www.intel.com/content/www/us/en/programmable/documentation/cru1439932898327.html*, (accessed on 20 December 2021).

[31] NIST, “Cryptographic standards and guidelines”, *online* *https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines*, (accessed on 10 December 2021).

[32] CSDITL, “Example values - cryptographic standards and guidelines”, *online* *https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/example-values*, (accessed on 19 December 2021).

[33] Y. Wu, J. P. Noonan, S. Agaian, *et al.*, “NPCR and UACI randomness tests for image encryption”, *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011, doi:10.1001/JSAT.2011.863-502-2.



Argyrios Sideris received his B.Sc. title in Computer Science in 2012, and he got his M.Sc. title in Pervasive and Mobile Computing Systems in 2017, both from the Hellenic Open University (HOU) of Patra, Greece. Since 2018 he has been a PhD candidate at the Department of Electrical and Computer Engineering at the Institute University of Western Macedonia (UOWM) of Kozani, Greece, and is conducting his research dissertation on "Security and cryptographic applications in embedded systems".

He is a student member at the Institute of Electrical and Electronics Engineers (IEEE), and his current research interests include Very-large-scale integration (VLSI) design and architectural design in field-programmable gate array (FPGA), cryptography and hardware security.

Theodora Sanida received her B.Sc. title in Computer Science in 2012 from the Hellenic Open University (HOU) of Patra, Greece. She got her M.Sc. title in Informatics Systems in Business Administration from the Department of Informatics and Telematics of the Harokopio University of Athens in 2016. Since 2018 she has been a PhD candidate at the Department of Electrical and Computer Engineering at the Institute University of Western Macedonia (UOWM) in Kozani, Greece. She is conducting her research dissertation on "Designing and implementing applications in heterogeneous computing".

She is a student member at the Institute of Electrical and Electronics Engineers (IEEE), and her current research interests include neural networks, machine learning, deep learning, cryptography and accelerators architectural design in field-programmable gate array (FPGA).

Dimitris Tsiktsiris received his Diploma Degree in Informatics and Telecommunications Engineering from the Faculty of Engineering of the University of Western Macedonia (2017). He is a PhD Candidate since 2018 at the department of Electrical and Computer Engineering at the University of Western Macedonia (UOWM) in Kozani, Greece.. He is a research associate at the Informatics and Technology Institute of the Centre for Research and Technology - Hellas since September 2019.

His primary research interests focus on computer vision using AI, deep learning algorithms, human activity recognition and acceleration on embedded systems and low-power devices.

Minas Dasygenis (Electric and Computer Engineer, 1999, Ph.D) is an Assistant Professor at the Polytechnic School of Kozani, Department of Electrical and Computer Engineering, University of Western Macedonia, Greece, in the research area of designing embedded systems and accelerators in homogeneous or heterogeneous architectures. He carries over 15 years of teaching experience in Operating Systems, Computer Architecture, Embedded Systems, Parallel & Distributed Systems.

His research interests are focused on computer architecture, robotics, embedded and cyber-physical systems, gamification, Internet of Things, security and hardware & software co synthesis. Currently, he is the Director of the Laboratory of Robotics, Embedded and Integrated systems, research coordinator in three programs, and supervises six PhD students.

Received: 30 March, 2022, Revised: 10 June 2022, Accepted: 11 June, 2022, Online: 18 July, 2022

DOI: https://dx.doi.org/10.55708/js0107005

A Review on Materials and Experimental Process used in Air-spring

Karnam Shri Harsh, Surbhi Razdan *

Mechanical Engineering, Dr. Vishwanath Karad MIT-WPU Faculty of Engineering, Kothrud, 411038, INDIA
* Corresponding author: Surbhi Razdan, Email - surbhi.razdan@mitwpu.edu.in

ABSTRACT: The present paper reviews an air spring, its types and construction, manufacturing process, testing and process of FEA analysis. Air spring is of three types - Sleeve-type air spring (SAS), Rolling-Lobe Air-Spring (RLAS), and Convoluted Air Spring (CAS). Spring stiffness is the main factor during manufacturing; to obtain it by FEA analysis and experimentation process is shown. The essential component is either Natural Rubber or Neoprene Rubber. To provide strength and reduce the chances of puncture, fabrics like Nylon and Polyester are reinforced with the rubber and vulcanised. This paper shows the process for obtaining and manufacturing these materials. Metals like Steel, Aluminium, and zinc alloy are also used in Air spring assembly.

KEYWORDS: Air spring, Stiffness, Rubber, Fibre, Materials

1. Introduction

An air-spring is a bellow made of rubber filled with gas. Air-spring provide a movable spring rate and have flexible load-bearing capacity. The use of pneumatics was started in the early 1900 when it was used as air suspension for the bicycle. It was the first when an air spring was introduced [1]. Slowly, the development of air suspension was seen in motorcycles in 2009 which was manufactured by a company Air Spring Ltd. A few years after the motorcycles were banned. In 1920 air suspension was introduced in automotive by George messier for his manufactured cars and provided air suspensions for aftermarkets.

US Government has also developed the air suspension for aircraft during the second world war to reduce their weight. Slowly, many companies started manufacturing air springs in different models that work in different forms. Mostly these air springs were seen in automobiles back then, but now we can see them as vibration insulators, actuators, laundry machines, textile looms etc. With the increase in the use, it is also required to know the capabilities of the air spring and its characteristics. They also have the advantages of providing adjustable height control and less friction. They are commonly used for vibration isolation and vibration control in suspension. They are also used in auxiliary suspension. The air-spring suspension system has an advantage over the conventional suspension system as it can counter the rollover effect due to crosswind conditions. The air spring framework is situated between the vehicle body and the bogie. Generally found in vehicle suspension frameworks, occasionally connected with a helical spring, they are likewise used to protect vibration in apparatus and as linear or angular actuators. Air springs are utilised using an air blower filling and emptying the air bladder. The load isn't distributed to the rubber liner. This liner just serves to contain the gas; the weight is connected to a cylinder or dab plate, which is upheld by the air within the bellow [2].

A self-in-out system is enough to keep the air spring's load stable; incidentally, a different loop is fused into the air inlet and outlet plan. Air springs have numerous unique benefits, for example- low cost, nearly constant natural frequency, ride comfort and road friendliness. Hence, air springs and machine isolators are generally utilised as a vehicular suspensions. They are also used as actuators in transfer stations, bark peeling machines, automotive ram weight adjustments etc. Many researchers have designed different models and designs of Air-springs. The essential components of an Air spring are as shown in Figure.

Construction

Air springs consist of the following components:

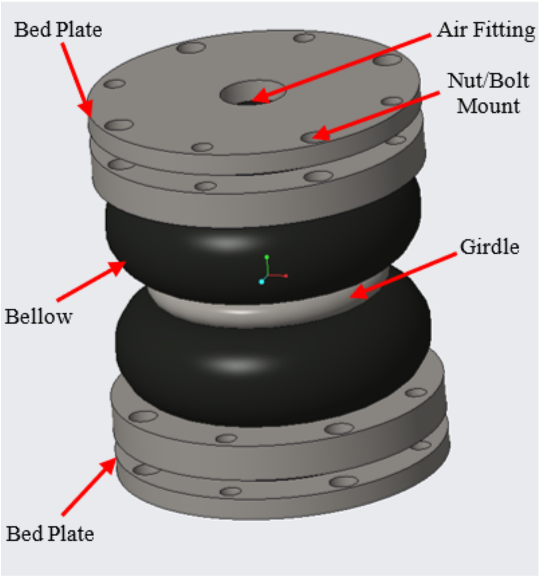


Figure 1: Components of Air-Spring

- **Air fitting -** A hole at the top of the air spring allows air in and out. If the spring is fully packed, it will lead to burst, and the spring will fail.
- **Nut/bolt mount -** During assembly, air spring is required to be fixed with other components for which nut/bolt mount is used.
- **Bead plate -** These are metal plates fixed rigidly on both sides of the rubber. These are mostly made of steel, zinc Alloy or Aluminium.
- **Bellows -** A multi-layer material filled with gas or air to withstand the load made up of neoprene or vulcanised rubber. These layers contain rubber and fabric. Fabric is used to make the rubber stronger. With the fabric and vulcanisation process, the stiffness of the rubber is increased.
- **Girdle –** This is found only in convoluted air springs to divide the rubber into two or three chambers.

Researchers have developed a wide variety of air-spring, explaining the various types and their applications.

Table 1: Types of Air-Spring **[3]**

Air Spring Types		
Sleeve-type air springs	Rolling-lobe air springs	Convoluted air springs
Sleeve-style air-springs consist of a member having a moulded bed inside. This design results in a smaller overall diameter. A bag of synthetic rubber compounds incorporates the internally mounted spring.	A single rubber cylindrical Bellow depending on its usage and load capacity, rolls outside while folding inside its rubber sheet. Its stroke length is high, and its strength is low.	Bellow springs possess mere lifting and load-carrying capacity. This type of air spring has multiple convoluted chambers and reinforced rubber. These types of springs are available in three configurations – Triple, double, and single chamber design.
Applications of SAS	Applications of RLAS	Applications of CAS
Light-duty trucks, Seat suspensions	Rail Vehicles, Heavy load Trucks & Trailers, Ambulance, Buses, Isolators & Actuators in Industries	Robotics - Pick & Place, Automotive Industries, Press machines, Conveyer system, Roll Tensioner, Tractor Suspension

2. Manufacturing and Materials

Air spring is manufactured to sustain and absorb sudden jerks and can be used for a long time. Replacing the air spring with a coil spring was the most significant challenge. The main element that plays a crucial role is the rubber below, a multi-layer material made of rubber and fabric. The natural rubber must be rolled into sheets, and required materials are mixed with rubber and passed through two rolling mills. The compound must be a homogeneous mixture as output [4]. Fabric is coated with this rubber sheet layer by layer in a sandwich pattern. Fabrics like Nylon and Polyester are used in the manufacturing of air springs. The rubber and fabric reinforcement increases the rubber's strength for spring [4], [5]. The bond between rubber and fabric should be strong. They should not get air bubbles between them. Generally, adhesives are used for bonding rubber with fabric.

Once the reinforced rubber is dried, it must undergo a vulcanisation process to increase its strength of reinforced rubber. Steel wires are placed between the layers of reinforcements at both ends of the bellows where the bead plate is clamped. Generally, this bead plate and girdle comprises steel, Aluminium, or zinc alloy.

The manufacturing of air springs usually consists of subsequent operations. Production of rubber, coating it to fabric layer, making a reinforced composite, vulcanisation of composite by high pressure and at high temperature, and then clamping it with metal bead plates at both ends.[6]

Rubber is the most crucial element of air spring; two types of rubber are used in all –

I. Natural Rubber
II. Neoprene Rubber

Natural Rubber – Hevea brasiliensis is the primary source of natural latex rubber. It belongs to the Euphorbiaceae family. Some more sources to extract the natural rubber are the Sapotaceae just family (gutta-percha) and Asteraceae families Parthenium argentatum (guayule rubber). The latex is a kind of milky liquid extracted from trees. This liquid contains rubber particles diluted to 15% and solidified with formic acid.[7] The solidified rubber material is passed through the rollers, which compresses the rubber removing water from it and making it into a sheet form. This sheet is later dried with hot air or smoke from the fire. The natural rubber has many grades, but the most distinguished latex and solid grade. We can obtain latex from trees, and the solid grade rubber is solidified in processing centres made of latex. The raw rubber and rolled rubber sheets are machined and milled in roller machines, reducing the molecular weight by breaking down the long chains of the polymer. Cis-1,4 polyisoprene is the chemical name for standard natural rubber and has the longest polymer chain. It has a small number of inorganic salts, lipids, proteins, and other materials. The natural rubber has long polymer chains which are coiled and entangled at room temperature.[8]

After making the rubber sheet, its tensile strength can be increased by the vulcanisation process. We can change the form of rubber from a thermoplastic state to elastomer material by mixing it with Sulphur and lead carbonate and heating this mixture. The reaction time of Sulphur and rubber is slow even at increased heat. To decrease this reaction time, accelerators are added with adhesives like antioxidants, fillers, and plasticisers. 3% weight of Sulphur is added to the rubber mixture and heated between 100 to 200º C during the vulcanisation or curing process. But if the % of Sulphur is increased, it will increase the cross-linking of the polymers, increasing the hardness of material and decreasing its flexibility. It requires 45% of Sulphur to harden the rubber fully. And by adding filler, the strength of the rubber can be increased. The most common filler used is carbon black, and to increase rubber's tensile strength, we should use fine-sized particles [7]

Table 2: Vulcanised natural rubber properties [9]

Tensile strength (Mpa)	17.239 to 24.13 Mpa
Elongation %	750 to 850 %
Density (Kg/m^3)	930 Kg/m^3
Recommended operating temperature (F)	-58 to 179.6 ºF

Properties of natural rubber

- It has high tensile and tear strength.
- It has good fatigue resistance.
- Excellent handling and tack strength
- It generates low heat as it has low hysteresis.
- Its rolling resistance is also low.
- It is resistant to tearing, chipping, and cutting.
- It is moderately resistant to heat, light, and ozone.
- It is less resistant to petroleum products – gasoline, naptha, and oils.
- The strength of natural rubber can be decreased in high temperatures.
- It is resistant to alkalies, salts and inorganic acids. [9], [10]

Neoprene Rubber - Neoprene rubber, often known as polychloroprene, is a synthetic substance made from polymerised chloroprene. Polychloroprene comprises carbon, hydrogen, and chlorine polymers cross-linked to provide neoprene features, including chemical inertness, heat, oil, water, and solvent resistance. Neoprene is made from acetylene which uses using catalyst converted into vinyl acetylene. The boiling point of vinyl acetylene is 5ºC and forms chlorobutadiene reacting with hydrochloric acid. Chlorobutadiene has a boiling point of 60 ºC. Primarily it is dangerous to the skin if splashed, and if soon be washed with water would still be harmful. Mixing chlorobutadiene with rosin, Sulphur is kept in soap solution and catalyst (salt) is added, which is agitated for two hours. This process gives us neoprene latex. Neoprene undergoes vulcanisation, which is the chemical treatment of synthetic rubber to enhance its properties, as part of its production process. Vulcanisation creates Sulphur bridges that connect individual chloroprene chains to form a larger molecule, resulting in cross-linking of molecules. The quantity of Sulphur links in a batch of neoprene impacts its overall qualities. As a result, depending on how chloroprene is vulcanised and how many Sulphur bonds are formed, neoprene can exhibit a wide range of characteristics without affecting its basic structure [11], [12].

We can get neoprene in different forms depending on the requirement and purpose they are –

- **Neoprene sheets**. They are useful for making protective gear like wet suits and gloves, but they may even be utilised for landfill liners or protective gear wraps.

- **Extruded neoprene.** Extrusions of neoprene are used as tubing or window sealing or split into gaskets, washers, or seals.

- **Neoprene foam.** Because neoprene foam is spongey and thick, it may also be utilised to cushion sporting equipment. It's also used to insulate industrial machinery and as a weather-stripping material [11].

Properties of neoprene rubber

- It is resistant to heat.
- It is also resistant to cold.
- It is compatible with materials like fabrics and metals.
- It can resist outside atmospheric conditions.
- It is resistant to chemicals and petroleum products as well [11], [12]

During characterization of rubber and elastomers it is essential to know that there are many standards available for testing process. Different types of tension, adhesion and com,pression tests standard are available for characterizing rubber and elastomers –

- ASTM D412 Tension Testing for Rubber and Elastomers
- ASTM D575 Compression Test of Rubber
- ISO 6133 Rubber Tear and Adhesion Strength
- ISO 34-1 & ISO 34-2 Tear Strength of Rubber, Vulcanized or Thermoplastic - Trouser

The Fabrics used for reinforcement are –

i. Nylon
ii. Polyester

Nylon – Nylon is a synthetic material with wide applications due to its transformable characteristics. They can quickly transform into fibres, moulded parts, and films. It also has biocompatible nature. It belongs to the polyamide family, which is a synthetic semi-crystalline polymer.

A polyamide is an amide group bonded with monomers which can either naturally or synthetically be obtained. Naturally, polyamides can be obtained from silk and wool. Synthetic polyamides can be manufactured through Nomex, Kevlar, and Perlon. Synthetic polyamide has three categories polyphthalamides, aromatic polyamide and aliphatic polyamide. Among these, we use semi-aromatic polyamide or aliphatic polyamide for making Nylon. Nylon can be used in many ways by providing a different shape and form by melting and then cooling. It has excellent mechanical properties, which can be further increased by adding other materials and elements. Nylon is used in the textile and food industries and is compatible with human tissues for biomedical implants [13], [14]

Properties of Nylon

- It is a thermoplastic material
- It is a semi-crystalline polymer and shows an amorphous phase after solidification.
- It is a good water absorbent.
- It is resistant to ultraviolet radiation.
- It is resistant to chemicals like alkaline and diluted acids.
- It undergoes Hydrolysis despite being chemical resistant.
- It is a Biocompatible material but can still be harmful and cause infections [14], [15].

Polyester - The common and widely used polyester fibre is polyethene terephthalate which is called PET, which is a synthetic fibre which is produced in huge quantities all over the world. It is a low-cost material and can be used with natural fabrics, which is also a recyclable material, providing convenience in processing and performance. This material has been very likely used on a large scale. Poly-ethylene terephthalate is a product of condensed ethyl Glycol and terephthalic. To successfully manufacture polymerised PET is purity in monomer and moisture-free vessel.

Table 3: Mechanical Properties of types of Nylon [14]

Property	Nylon 6 (toughened)	Nylon 6 (fiber)	Nylon 6 (30 % carbon fiber)	Nylon 66 (toughened)	Nylon 11 (rigid)	Nylon 11 (flexible)	Nylon 12 (rigid)	Nylon 12 (flexible)
Density (kg/m3)	1070–1100	1130–1150	1260–1280	1060–1080	1020–1040	1040–1050	1000–1020	1030–1040
Young's modulus (GPa)	0.782–0.976	4–5	12.9–16.1	0.939–1.17	1.06–1.33	0.35–0.36	1.08–1.35	0.35–0.42
Yield strength (MPa)	33.1–41.3	600–1050	131–163	36.1–45.1	35.4–44.1	25–27	34.8–43.4	22–25
Elongation (%)	37.2–53.5	16–19	3.01–4.33	41–59	280–320	360–430	41–59	360
Fatigue strength (107 cycles) (MPa)	40.3–44.5	–	55.9–61.7	17.6–19.4	20–22	18–20.4	19–21	16
Toughness (kJ/m2)	9.72–13	–	1.83–2.45	8.72–11.7	8.07–10.8	18.9–19.5	8.01–10.7	16.7–20.2
Humidity absorption @ sat (%)	2.1–2.9	4 – 4.5	2–2.6	1.8–2.4	0.68–0.92	0.9	0.62–0.84	1.2–1.4

To make fibre from the polymer, it must be melted down or put into the spinning machine after it achieves the required molecular weight. Obtaining fibre from a spinning machine is called continuous polymerisation. Further PET pallet's molecular weight can be increased by solid-state polymerisation. At about 160ºC PET chip is dried, crystallised, and heated below the melting point. This process is done in extreme dryness and vacuum [16], [17].

Properties of polyester

- Polyester's thermal and mechanical properties can be affected or changed by the degree of crystallin.
- Crystallinity and orientation of molecules can increase young's modulus and break the tension, decreasing break elongation.
- It is resistant to organic acids.
- It is resistant to weak alkaline and partially resistant to strong alkaline.
- It is resistant to oxidant agents such as soaps, bleach, detergent, etc.
- It is resistant to ultraviolet radiation, but its fabrics can get weaker if exposed for a more extended period [17]

Table 4: Physical properties of polyester PET [18]

Crystal habit	Triclinic: one polymer chain per unit cell
Cell parameters	a = 0.444 nm; b = 0.591 nm; c = 1.067 nm, α = 100 degrees. β = 117 degrees; γ = 112 degrees
Cell density	1.52 g/cm3
T_m (DSC)	260ºC-265ºC
ΔH_f	140 J/g; 33.5 cal/g
T_g (solid chip)	79ºC (DSC)
T_g (drawn fiber)	120ºC (dynamic loss)
Specific gravity	1.33 (amorphous, undrawn), 1.39 (crystalline drawn fibre)

The metals used for clamping are made of –

i. Steel
ii. Zinc Alloy
iii. Aluminium

Steel – Steel is an alloy of Iron and carbon with a carbon of 2%, and if the percentage of carbon increases, it is known to be cast Iron. Steel is a widely used material all over the world in many wide ranges of application as construction, mechanical tools, machines, needles etc. Steel is produced by two methods Basic Oxygen Furnace or Electric Arc Furnace. Steel has four types – Carbon Steel, Alloy steel, Stainless steel, and Tool steel [19]

Table 5: Properties of steel for above four types [20]

Properties	Carbon Steels	Alloy Steels	Stainless Steels	Tool Steels
Density (1000 kg/m3)	7.85	7.85	7.75-8.1	7.72-8.0
Elastic Modulus (GPa)	190-210	190-210	190-210	190-210
Poisson's Ratio	0.27-0.3	0.27-0.3	0.27-0.3	0.27-0.3
Thermal Expansion (10-6/K)	11-16.6	9.0-15	9.0-20.7	9.4-15.1
Melting Point (°C)	1371-1454			
Thermal Conductivity (W/m-K)	24.3-65.2	26-48.6	11.2-36.7	19.9-48.3
Specific Heat (J/kg K)	450-2081	452-1499	420-500	
Electrical Resistivity (10-9W-m)	130-1250	210-1251	75.7-1020	
Tensile Strength (MPa)	276-1882	758-1882	515-827	640-2000
Yield Strength (MPa)	186-758	366-1793	207-552	380-440
Percent Elongation (%)	10-32	4-31	12-40	5-25
Hardness (Brinell 3000kg)	86-388	149-627	137-595	210-620

Aluminium – Aluminium and its alloys are widely used in industries due to its suitable physical, mechanical and tribological properties. It is the third most common metal in the earth's crust. It has FCC type structure which is ductile at ambient temperature, which makes it easily machinable. It has a lower melting temperature than other engineering metals. Aluminium is found in two states after production – the primary and alloy states. Aluminium alloys are used in aerospace and automotive industries as they can replace steel and Iron due to their promising strength-to-weight properties [21]

Table 6: General properties of Aluminium [22]

Density (kg/m^3)	2.5 x 10^3 to 2.9 x 10^3
Yield strength (Pa)	3 x 10^7 to 5 x 10^8
Tensile strength (Pa)	5.8 x 10^7 to 5 x 10^8
Elongation (%Strain)	0.01 - 0.44
Hardness (Pa)	1.18 x 10^8 to 1.48 x 10^9
Melting Temperature (ºC)	475 to 677
Fracture Toughness (Pa/m$^{0.5}$)	2.2 x 10^7 to 3.5 x 10^7
Young's Modulus (Pa)	6.8 x 10^{10} to 8.2 x 10^{10}

Characteristics of Aluminium –

- Aluminium is light weighted.
- It is a durable material.
- It is corrosion-resistant.
- It can be easily machined
- It doesn't have magnetic nature
- It is an electric and heat conductor.
- It possibly has a wide range of surface treatments.[22], [23]

Zinc Alloy – Zinc is the next most used metal after iron, Aluminium and copper. Primarily zinc is used for removing corrosion and galvanising. Using zinc for galvanising increases iron and steel recyclability. Brass is the zinc and copper alloy with adding some tin and alloy. Previously zinc was obtained from zinc oxide ores, but sulphide ore was also discovered later, which is in large quantity present on earth, so after this sulphide ore is discovered, zinc is also produced from zinc sulphide.[24]

Table 7: Properties of zinc alloy [25]

Density (g/cm^3)	6.3
Elastic modulus (GPa)	86
Tensile strength (MPa)	370
Elongation (%)	8
Heat transfer rate (W/(m·K))	120
Melting point (°F)	716
Coefficient of thermal expansion (K-1)	2.3 ✕ 10-5
Yield strength (MPa)	290
Electrical conductivity (S/m)	1.624 * 10-8

3. Vulcanization Process

The process of vulcanisation is an important part when it comes to the use of rubber for goods. When we use rubber for tires and spring-like air products, or can say mechanical products which require strength, vulcanisation is necessary. Without it, rubbers don't have the strength to regain their original shape when a high load is applied. The temperature required for the vulcanisation process is about 140° -180°C.

4. Testing and analysis of Air Spring

Stiffness Test

Stiffness- Stiffness is the resisting force of an object when an external force is applied to it. In other words, materials with more flexibility have less stiffness. Stiffness can be calculated by –

$$K = \frac{F}{\delta}$$

We can use FEA (Finite Element Analysis), Experimental process and calculations to calculate the stiffness of the air spring. Many researchers have come up with different ways to obtain the vertical stiffness of air springs.

Most of the stiffness of the spring is based on the air inside the rubber bellows. So, the stiffness of spring is sum of the stiffness of air column inside the spring and the stiffness of rubber bellow.[26]

FEA Analysis

For the analysis of an air spring, we must mainly consider two points, the air conditions or can say air pressure inside the spring and the second is the meshing elements of the model.

FORTRAN – It is a coding language software in which we can write the programs and can develop FEM code which can handle the contact problem for incompressible rubber part analysis.[27]

ABAQUS – It gives a tremendous feasible result in boundary conditions of the air. In ABAQUS programming, the component type FAX 2 can be chosen, which supplies an extra degree 8 to assess the inside pressure of the airbag. Also, during the deformation of the airbag, mainly the elastic material distorted intensely, the meshing may be done in the ANSA programming to ascertain a right and concurrent outcome.[28]

ANSA - It is a unique software used for pre-processing and for meshing. Unlike other software, we can have a good association between CAD models and the mesh created in ANSA.

ANSYS – ANSYS is user-friendly software. One can import the geometry from CAD software and can work in ansys with ease. We can add materials properties of rubber in engineering data and rest boundary conditions in the model window.

Boundary conditions needed to apply are the base of the air spring should be fully fixed and force applied from the top.

Test process

Before proceeding, it is necessary to know the basic process for obtaining the stiffness of an Air spring. The Air spring must be placed on a flat surface and clamped rigidly, allowing the spring to get into an equilibrium state and record the height. Add weights and record the changes in height. Then, the stiffness can be calculated by the relation between force and deflection.[29]

Stiffness can be calculated based on mathematical models and algorithms derived from explicit and implicit algorithms.[30] We can use Universal Testing Machine for experimentation. Clamping air spring in both the jaws of UTM and leaving it to get in an equilibrium state. By providing the load to the electrical UTM machine, we can get the deflection of the air spring, and by calculating the relation of force and deflection, we can get the stiffness value [31], [32].

A blast test can be performed by mechanically assembling the test machine, which requires the top and bottom of the spring to be fixed and the pressure inside the spring to be increased. The blasting pressure for an air spring should be three times that of the normal pressure of the spring. To get this during experimentation, it is recommended to use fluid and create the pressure required for the test [6].

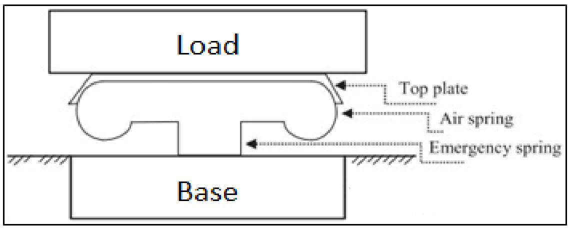


Figure 2: Schematic of Experimental setup

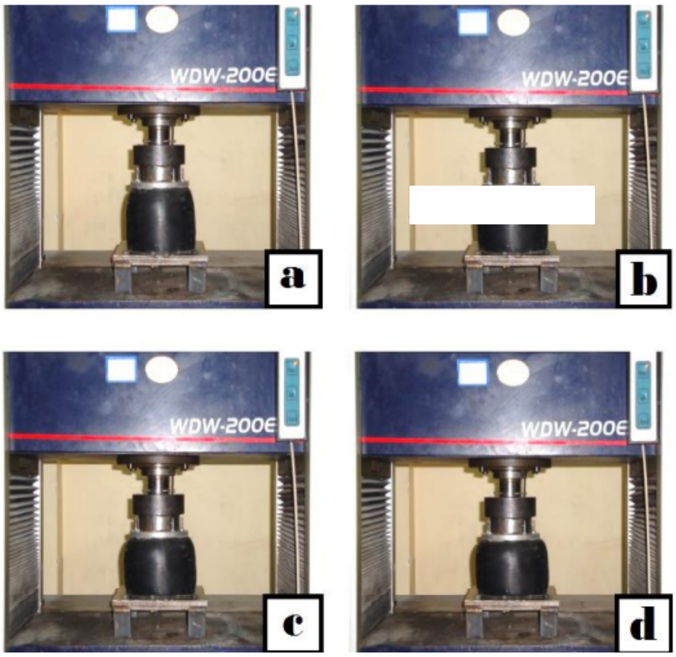


Figure 3: Loading stages of the inflated air-spring pressurized with 0.1 MPa (a) at free height, (b) displaced 5 mm, (c) displaced 10 mm, (d) displaced 15 mm.

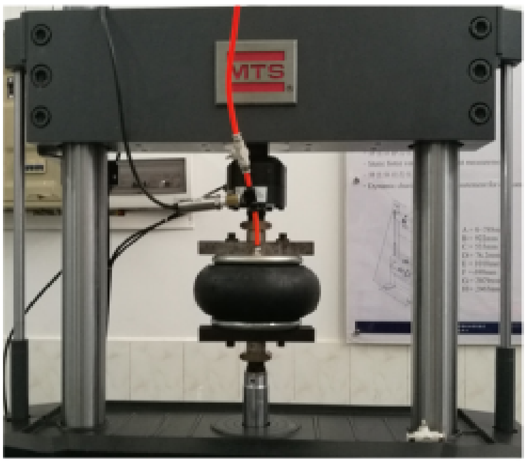


Figure 4: Testing of single bellow air spring in MTS UTM

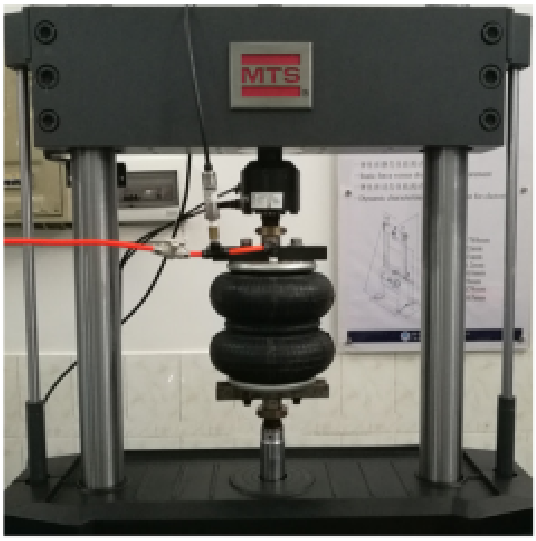


Figure 5: Testing of double bellow air spring in MTS UTM

In figure 2 it is shown the setup required for stiffness calculation of an Air-spring Displacement of the spring is calculated by applying load at its top and the bottom should be fixed. Based on this some researches have tested air-springs. These experimental setups are shown below.

These setups shows that the UTM machines are mostly used as experimental setups for testing stiffness. Where as for blast test the setup is same as the above but instead of applying load we have to fix both the sides of air spring and should add pressurized water to it.

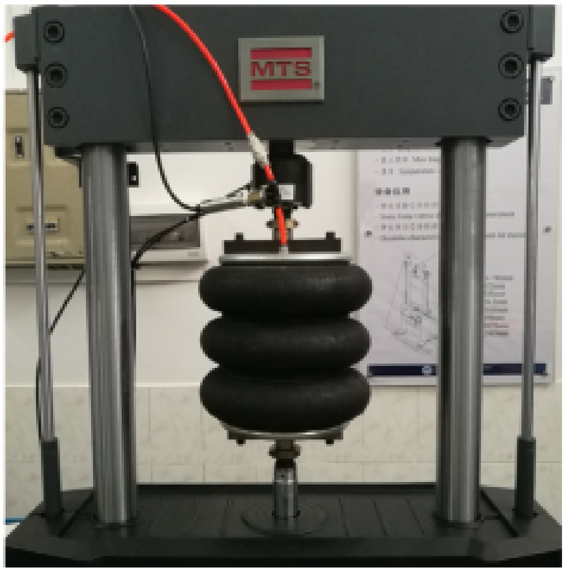


Figure 6: Testing of triple bellow air spring in MTS UTM

5. Conclusion

A properly designed air spring should have a low vertical stiffness for improved low-frequency vibration isolation and a significant high one to reduce suspension compression under static load. FEM can reduce the effort of experimental analysis. The results of FEM are reliable. Both experimental and analytical process for vertical stiffness gives correct results. Tables and Figures can be single or double columns for double-column use section breaks.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] ARCHIBALD SHARP, WILLIAM THOMAS SHAW – "Improvements in Cycle" GB190100764A – 1901

[2] Pak Kin Wong, Zhengchao Xie, “Analysis of automotive rolling lobe air spring under alternative factors with finite element model,” *Journal of Mechanical Science and Technology*, vol. 28, no. 12, pp. 5069-5081, 2014, doi: 10.1007/s12206-014-1128-9.

[3] un-Jie Chen, Zhi-Hong Yin, Subhash Rakheja, Jiang-Hua He, Kong-Hui Guo, "Theoretical modelling and experimental analysis of the vertical stiffness of a convoluted air spring including the effect of the stiffness of the bellows," *Proc IMechE Part D: J Automobile Engineering*, vol. 232, no. 4, pp. 547-561, 2017, doi:10.1177/0954407017704589.

[4] Dr. Mohsin Noori Hamzah, Mahmood Shakir Nima, "Experimental and Numerical Investigations of an Inflated Air-Spring Made of Fiber-Reinforced Rubber," *Al-Qadisiyah Journal for Engineering Sciences*, Vol. 8, no.3, pp. 355-368, 2015.

[5] Hongguang Li, Konghui Guo, Shuqi Chen, Wei Wang, Fuzhong Cong, "Design of Stiffness for Air Spring Based on ABAQUS", *Mathematical Problems in Engineering*, vol. 2013, pp. 1-5, Article ID 528218, doi:10.1155/2013/528218.

[6] Burhan Sarıoglu, Ali Durmus, "Manufacture and Testing of Air Springs Used in Railway Vehicles," *Arabian Journal for Science and Engineering*, vol. 44, no. 9, pp. 7967-7977, 2019 doi:10.1007/s13369-019-03981-w.

[7] http://www.industrialrubbergoods.com/natural-rubber.html - Natural rubber

[8] Thoguluva Raghavan Vijayaram – "A TECHNICAL REVIEW ON RUBBER," *International Journal on Design and Manufacturing Technologies*, Vol.3, No.1, pp. 25-37, 2009.

[9] C. Harris, A. Piersol, Harris, *Mechanical properties of rubber*, shock and vibration handbook 5th edition chapter 33, , McGraw-Hill, 2002.

[10] Marie-Noëlle Crepy, Donald V. Belsito, *chapter 67 Rubber* Kanerva's Occupational Dermatology, Third Edition, Springer 2020

[11] https://www.thomasnet.com/articles/plastics-rubber/traits-applications-neoprene/ - Neoprene rubber

[12] E. R. BRIDGWATER, E. I. du Pont de Nemours & Companq-, Inc., Wihnington, Del, "Neoprene, The Chloroprene Rubber," *Industrial and Engineering Chemistry*, vol. 32, no. 9, pp. 1155-1156, doi:10.1021/ie50369a004.

[13] I M Hanif, M R Noor Syuhaili, M F Hasmori, S M Shahmi, "Effect of nylon fiber on mechanical properties of cement based mortar",” 2017 *IOP Conf. Series: Materials Science and Engineering*”, vol. 271, pp. 1-7, doi:10.1088/1757-899X/271/1/012080.

[14] Mohamadreza Shakiba, Erfan Rezvani Ghomi, Fatemeh Khosravi, Shirzad Jouybar, Ashkan Bigham, Mina Zare, Majid Abdouss, Roxana Moaref, Seeram Ramakrishna, "Nylon—A material introduction and overview for biomedical applications" *Polymers Advanced Technologies*, vol. 32, no. 9, pp. 3368-3383, 2021, doi:10.1002/pat.5372.

[15] David J. Barillo, Morano Pozza b, Mary Margaret-Brandt, "A literature review of the military uses of silver-nylon dressings with emphasis on wartime operations," *Elsevier: burns*, vol. 40, no. 1 pp. 24–29, 2014, doi:10.1016/j.burns.2014.09.017.

[16] Asnake Ketema, Amare Worku, "Review on Intermolecular Forces between Dyes Used for Polyester Dyeing and Polyester Fiber" *Journal of Chemistry* vol. 2020, article ID 66284 04, pp. 1-7, doi:10.1155/2020/6628404.

[17] S. M. HANSEN P. B. SARGEANT E. I. du Pont de Nemours & Co., Inc.- "*Fibers, Polyester*" - Kirk-Othmer Encyclopedia of Chemical Technology. 1st ed., vol. 13, pp. 840–847, 2000, doi:10.1002/0471238961.1615122508011419.a01.

[18] Michel Jaffe, Anthony J. Easts, Xianhong Feng, “8-Polyester fibers,” *Thermal Analysis of Textiles and Fibers*, woodhead Publishing, Elsevier 2020, pp. 133-149, doi:10.1016/B978-0-08-100572-9.00008-2.

[19] Edward F. Wente, “Steel” *Encyclopedia Britannica*, 2019, https://www.britannica.com/technology/steel.

[20] Steel & Steel Alloy Stamping, Trident components, https://www.tridentcomponents.com/steel-stamping/.

[21] H.A. Elhadari, H.A. Patel, D.L. Chena, W. Kasprzak, "Tensile and fatigue properties of a cast aluminum alloy with Ti, Zr and V additions," *Materials Science and Engineering: A*, vol. 528, no. 28, pp. 8128–8138, 2011, doi:10.1016/j.msea.2011.07.018

[22] https://dielectricmfg.com/knowledge-base/aluminum/ - Aluminium

[23] ND. Alexopoulos, Sp.G. Pantelakis – "Quality evaluation of A357 cast aluminum alloy specimens subjected to different artificial aging treatment" *Materials and Design*, vol. 25 no. 5 pp. 419–430, 2004, doi:10.1016/j.matdes.2003.11.007.

[24] Annalisa Pola, Marialaura Tocci, Frank E. Goodwin, "Review of Microstructures and Properties of Zinc Alloys," *Metals*, vol. 10, no. 2, pp. 1-16, 2020, doi:10.3390/met10020253.

[25] https://matmatch.com/learn/material/zinc-alloy - “Zinc Alloys: Properties, Production, Processing and Applications,” Matmatch.

[26] Jiatong Ye, Hua Huang, Chenchen He, Guangyuan Liu, "Analysis of Vertical Stiffness of Air Spring Based on Finite Element Method",” *2018 MATEC Web of Conferences*, vol. 153, article no. 06006, 2017, pp.1-5, doi:10.1051/matecconf/201815306006.

[27] Tamas Mankovitsa, Tamas Szabób, “Finite Element Analysis of Rubber Bumper Used in Air-springs,” *Procedia Engineering*, Elsevier, vol. 48 pp. 388 – 395, 2012, doi:10.1016/j.proeng.2012.09.530.

[28] Jian Sun, “Calculation of Vertical Stiffness of Air Spring with FEM”,” *2011 In Greece: 4th ANSA & μETA International Conference*, 2011

[29] Surbhi Razdan, P. J. Awasare, Suresh Y. Bhave, "Active Vibration Control using Air Spring," *J. Inst. Eng. India Ser. C* vol. 100, no. 1, pp. 1-12, 2019, doi:10.1007/s40032-017-0424-4

[30] XU Wei, HE Lin, SHUAI Chang geng and YE Zhen xia, "Stiffness Calculation and Dynamic Simulation of Air Spring" *International design engineering technical conferences & Computers and Information in Engineering Conference*, pp. 1395-1399, 2005, doi:10.1115/DETC2005-84338.

[31] Jun-Jie Chen, Zhi-Hong Yin, Xian-Ju Yuan, “A refined stiffness model of rolling lobe air spring with structural parameters and the stiffness characteristics of rubber bellows,” ELSEVIER-*Measurement*, vol. 169, pp. 1-14, 2021, doi:10.1016/j.measurement.2020.108355.

[32] Di Qu, Xiandong Liu, Guangtong Liu, Yifan Bai1, Tian He, "Analysis of vibration isolation performance of parallel air spring system for precision equipment transportation," *Measurement and Control*, Vol. 52, no. 3-4, pp. 291–302, 2019, doi:10.1177/0020294019836122.

K. Shri Harsh is currently pursuing his master's degree in Mechanical CAD/CAM/CAE from Dr. Vishwanath Karad MIT World Peace University from, Pune, Maharashtra, India. He had completed his bachelor's degree in Mechanical Engineering from Kalinga University, Naya Raipur, Chhattisgarh. His current research includes Air-Spring with natural fabric.

Dr. Surbhi Razdan is currently working as an Assistant Professor in the School of Mechanical Engineering, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India. She has published 12 research papers. She has 2 patents granted and 2 of her patents have been published.

Received: 21 April, 2022, Revised: 19 June 2022, Accepted: 27 June, 2022, Online: 18 July, 2022

DOI: https://dx.doi.org/10.55708/js0107006

Advanced Medical Telemonitoring for the Suspected Cases of Covid-19 Virus

Mohamed Touil *, **Lhoussain Bahatti, Abdelmounime El Magri**

IESI Laboratory, ENSET Mohammedia, Hassan II University of Casablanca, Morocco
*Corresponding author: Mohamed TOUIL, Email: touilenset@gmail.com

ABSTRACT: Nowadays Corona Virus is threatening everyone, everywhere because it extremely dangerous. For many reasons; the first one it is a contagious virus, the second reason is there is no definite vaccination for that, because even some vaccinated people against Covid were affected. in the same regard this paper will present a telemedicine solution against Covid-19. the solution contains two parts. One is software, it represents a platform for real-time medical telemonitoring and also some important statistics are performed there. The other part is hardware, it lies on the usage of remote sensors like the temperature sensor the location sensor and so on, to acquire the vital parameters of the affected covid cases. And will have a wearable sensor network Also, there are many computers where we install the different parts of the platform in order to acquire patients' data and performing statistical studies as well. For that purpose, the LabVIEW software is used to develop different interfaces. Those sensors are connected to the platform in a wireless method, and all data processing are performed on the computers. The proposed solution will manage the whole country because there are local servers and also a main server to perform statistics and help the government to make the proper decision for example total lockdown partial lockdown etc.

KEYWORDS: COVID 19, Telemedicine, Wearable Sensors Network, Statistical Studies, Medical Telemonitoring

1. Introduction

So far Covid -19 affected a lot of people over the world, by the first of June 2022 the world situation known more than 500 million of affected cases, and more than 6 million of deaths. And during this period of time each country has made its proper decision. Inevitably there is a difference between countries. Because the number of affected cases depends on many things. The first one is the strategy of each country against Covid-19, the second one is the immunity system of each race of people and finally the conscience of people. the world organization (WHO) is publishing continuously a plenty of news every day. Consequently, we came to know that the symptoms start between 1 and 14 days of infection. And since that virus is contagious everyone can affect everyone. Hence the suspected case must stay away from other people for at least 14 days [1]. In this regard may researchers has performed many studies in the aim of fighting against Corona virus or at least reduce it spread. Some of them used predictive algorithm [2], others were trying to develop new vaccines [3] and so on.

In our paper we proposed a telemedicine platform for two aims, firstly to remote the vital parameters of the suspected and the affected cases by covid-19 using wearable sensors network handled by each suspected or infected case, secondly to manage the covid situation in terms of public authorities' decision, in other words our platform will perform statistical analysis in real-time and everywhere in the country. And it will help the government to make the proper decision. The medical telemonitoring will significantly reduce the direct contact between the healthcare professional and the patient, then the infection will be reduced immediately. On the other hand, the suspected person can take the small device that contain sensors and leave the hospital after 30 minutes, and will be remotely monitored at home instead of staying in the hospital [4].

When the patient comes to the hospital, first must be isolated for a period of 14 days, if the temperature of that patient is increased during this period, the medical staff must perform the PCR test otherwise after 14 days they do it. If this patient is confirmed, then the healthcare staff must proceed with the drugs. And if the person is not confirmed after 14 days, he/she must leave the hospital, the figure below illustrates the diagram of the process of the patient inside the hospital.

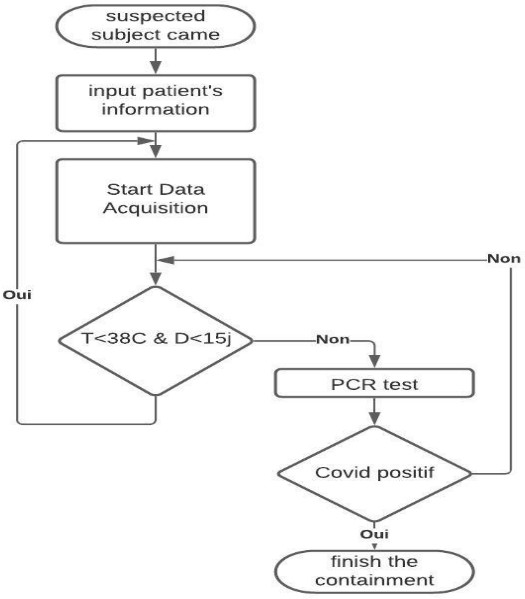


Figure 1: The process of the suspected patient inside the hospital

Recently several researchers and engineers in science technology area started to perform a plenty of studies about wireless wearable sensors. The first application was in the industrial field such as the telemonitoring of industrial parameters. And the production line. And after those biomedical engineers moved to the medical telemonitoring of patient, by acquiring remotely the vital parameters like the Electrocardiogram (ECG), the human body temperature, the noninvasive pressure (NIP) etc. [5] [6]. and so far, the wearable sensors network became very powerful solution for the medical data monitoring. In the same regard our paper will mention about a digital platform to perform the medical telemonitoring of the suspected or the infected cases of covid-19. This platform allows us to also to perform statistics in real-time for lot of people in the same time and with different locations. This platform also is able to display the vital parameters of a specific patient and store all data in a main server. The vital parameters that will be monitored are decided as the main symptoms of corona virus.

Our paper will be organized as follow:

Section 1: is an introduction of the paper.

Section 2: describes the platform layout and details each part of this last.

Section 3: illustrates the proof of concept of our project.

Section 4: concerns result and the interpretation.

2. Platform Layout Description

To develop our platform, we used LabVIEW software to present different interfaces. because this is just a prototype otherwise, we need to consider about many things like the integrity of the medical data, the cybersecurity, medical data privacy etc. but our first aim remains the medical telemonitoring, the other features can be enhanced later.

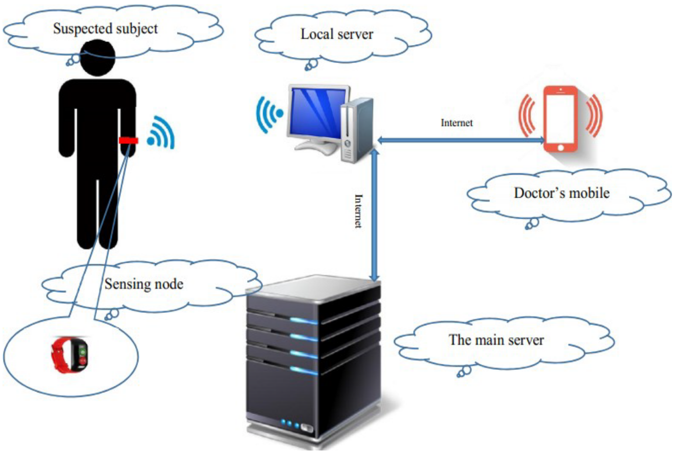


Figure 2: Architecture of the information system with WSN

The figure 2 illustrates the architecture of the whole platform:

- The sensing node represent all the sensors such as temperature, ECG, location. That item acquires all values and sends them remotely to the local server in the hospital for the preprocessing, storing and sending to the main server afterwards.[6]
- The local server is the computer located in each hospital; it is responsible for the real-time analysis of all the acquired medical parameters. It detects the high temperature, the patient's location if there are any changes. At the end of each period of time determined by the user will send all data and statistics to the main server. The doctor's phone also will be notified from that local PC.
- The doctor or the healthcare professional in the hospital will receive the notification associated with the patient info is there is any abnormal parameter change. Immediately he will check the patient status and he will confirm the case from his mobile phone. After all the confirmations will be sent to the main server for statistical purposes.
- The main server has two important roles, firstly the statistical study for the whole country is being performed here. Secondly that main sever helps the public authority to make the right decision for citizens. If they can move and practice their daily activities without limit or some precautions must be taken.

And since corona virus is strongly contagious, our proposed platform will reduce extremely the direct contact in the hospital especial between doctors, healthcare professional and patients as well.

3. The Proof of Concept

To perform the proof of concept, we chose some didactic sensors some of them are certified but others no.

- NodeMcu for wireless data transmission [6].
- Temperature sensor DHT11 to acquire the human body temperature [7].
- Location sensor for tracking the patient.
- 2 Workstations as the local server and the main server.
- Cables for connecting the different items.

3.1. Materials Specifications

- DHT11 specifications is presented in Table 1.

Table 1: *DHT11 Specifications*

Specification	Value
Resolution	16 Bit
Repeatability	±1 °C
Accuracy	25°C ±2°C
Response time	1/e (63%) 10s
Power supply DC	3.3□ 5.5V

- Workstations:

To carry out our prototype we used two laptops with the following spects: CPU: core™ i5-7200U 2.50GHz (4cpu); RAM: 8192Mo.

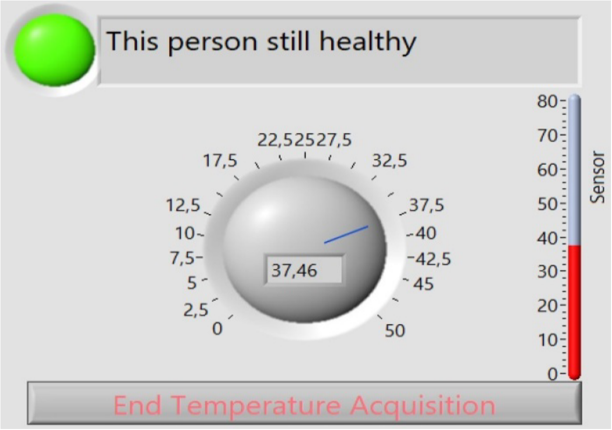
The figure (3) shows the simulation of the developed interface using LABVIEW with normal and abnormal temperature value.

3.2. Data processing algorithm

- Temperature processing

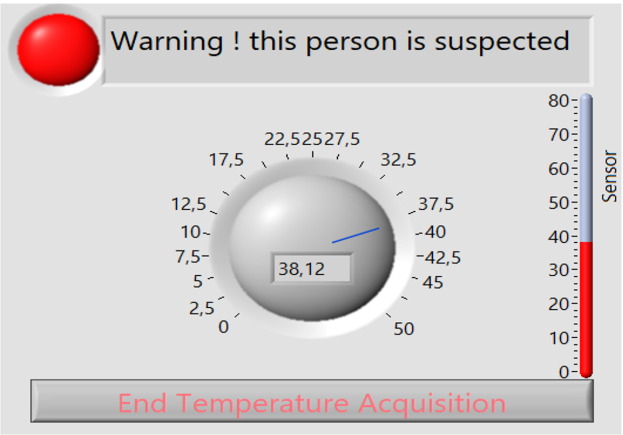
For the medical data processing there are three main phases, firstly data acquisition, in which we take the needed data but with all the measurements noises and artifacts, fortunately for temperature there is no possible artifacts if we measure from the proper region. Secondly data cleaning or denoising in order to remove all the artifact and keep only the useful part of the signal and the precision of this stage will significantly affect the quality of the next step. Thirdly data classification in this phase we check if the medical parameter is in the normal range or not. our focus in this section the human body temperature. The normal value of this last is 36.66, but this value is changing by the time [7] have performed one important study after several years they discovered that the average human body temperature is 36.11°C and not 36.66°C [7]. According to the CDC (centers for disease control and prevention) a person is considered has a fever when his/her temperature is greater than 38°C. so our platform calculation is taking 38°C as a threshold value. If the suspect case get a high temperature. The covid test must be performed immediately in order to confirm his infection.

The figure (3) illustrates the simulation of the developed algorithm with normal and abnormal temperature value



This person still healthy

Figure 3: The detection algorithm interface 1.



Warning ! this person is suspected

Figure 4: The detection algorithm interface 2.

This patient's body temperature is in the normal range so according to covid19 symptoms this subject is healthy.

As described in the introduction section our aim is to detect the suspected cases affected by coronavirus. That is why when the person's temperature is out of the normal range, other analysis must be done in order to be confirmed.

In the previous program, we change the temperature manually for simulation purpose. In bellowing figure (6) two programs are used MATLAB and LabVIEW and the temperature value is changes randomly in order to test the efficiency of our algorithm [8]. The generated values are used as the connected sensors to the platform.

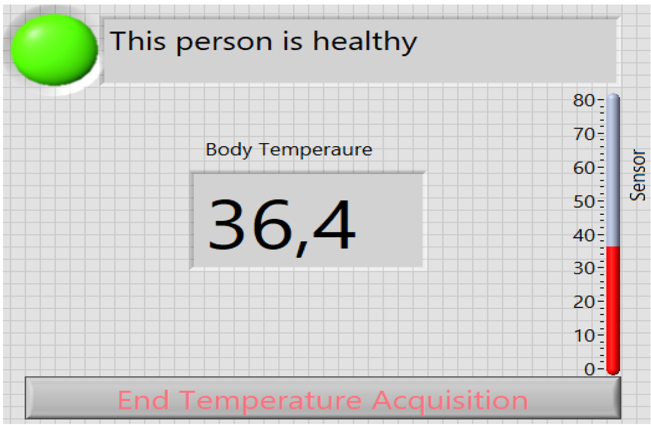


Figure 5: The detection algorithm –front panel.

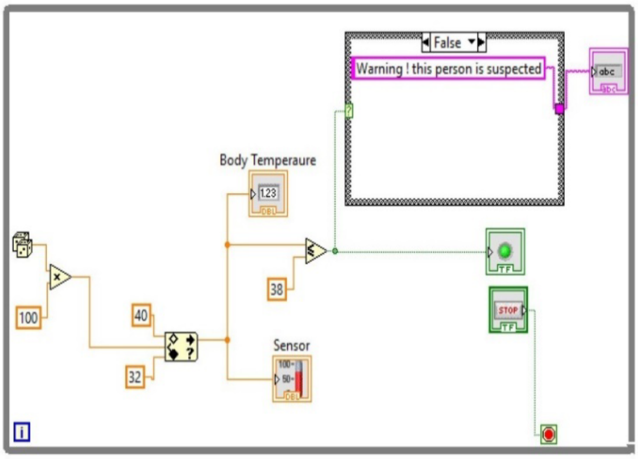


Figure 6: The detection algorithm –block diagram.

In the platform database, our elements are the sensing nodes. Each node has the information below:

- The unique ID is the CIN/passport number,
- The patient name,
- The patient age,
- The patient's condition.

3.3. *Information system*

In the information system the subject or the patient will be identified by three elements:

- The subject's name
- The CIN/ passport number
- The patient's location

According to the temperature changes, the subject will be confirmed as a covid19 suspected case or not, that is why this platform will communicate in real-time with the sensing node [8], in order to get the related parameters such as the location and the temperature.

As we are in the proof-of-concept step, "Thingspeak" cloud space is used for online temperature recording [9]. The figure bellow illustrates the recorded temperature using the NodeMcu module and temperature sensor [9].

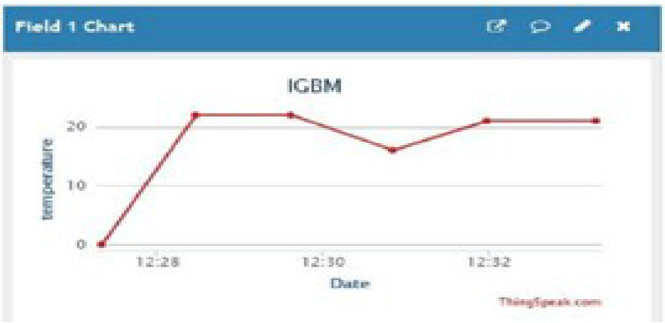


Figure 7: Cloud processing and storage interface

We used Thingspeak cloud space because at the same time, it allows us to collect data from different sensors [9] and analyze the collected data using MATLAB software. So, we can perform many statistical studies using the same platform, such as high temperature detection and the number of confirmed suspected persons, etc.

According to the temperature of each patient the bellowing table will be displayed on the main server [10].

Table 2: Local Server Data processing

CIN	Name	City	Status
A22020	Alami	Rabat	healthy
A25252	Saadani	Rabat	suspect
C52458	Ghita	Casa	recovered

Another table will be displayed below for the statistical purpose, in order to have an idea about the spread rate for each city [11].

Table 3: Main Server Data processing

City	confi	recove	death	rate
Rabat	511	300	18	15%
Casa	1500	1200	75	25%

N.B: all data in the previous table are random values just to highlight the proof of concept.

- ECG signal processing

The ECG signal processing is a long story even though we will mention about the main processing steps in order to calculate the heart rate of the patient in real-time. As it is known among the electrophysiology data analysts, the first there are three stages of ECG signal processing as follow:

1. The signal cleaning**:** in this stage, we have to remove all the noises and keeping only the useful part of the signal. There are two kinds of noises, the first one is related to the patient like the breathing, the baseline, the interference of the other physiological signals like the EMG, etc. the second type of noise is related to the

patient itself. Such as the white noise, the power supply frequency, etc. to remove all kinds of noises there are several methods, the classical filter like the high pass filter, the band pass filter and so on but also there is the wavelet method and the blind separation method. The most important thing is to remove only the noise components and keeping the desired part of the signal. We focus on that purpose because some filtering methods may destroy the useful part of the signal. The figures below illustrate different cleaning operations that were performed during this work during the cleaning process three kinds of filters were used, the notch filter to remove the power supply frequency, the "Detrend" function of MATLAB to delete the linear part of the baseline and the polynomial interpolation to remove the nonlinear component of the baseline[12].

2. <u>ECG features extraction:</u> in our case, we extract only the heart beats, in order to detect in Realtime the state of the heart if it is beating in the normal range or not. for most of people the normal cardiac frequency range is between 60 and 100 beat per minute (Bpm).
3. <u>ECG signal Classification:</u> this is the final stage of ECG signal processing in our case. That to say, after the cleaning and the features extraction we decide accordingly, it means to classify signals and we classify the suspected patient afterwards.

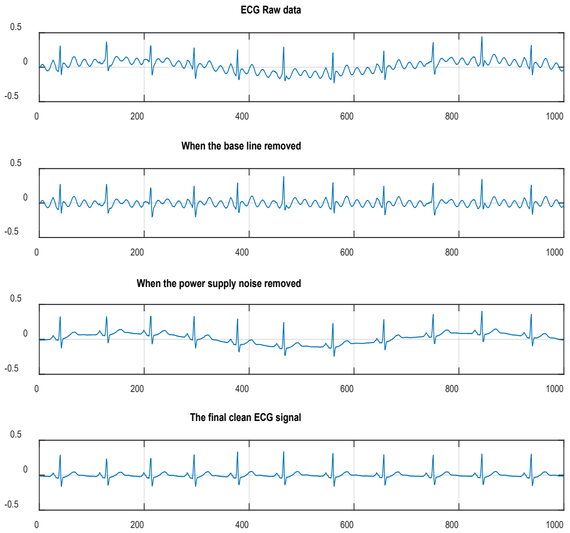


Figure 6: ECG Signal Cleaning

4. Results & Interpretation

Our platform of medical telemonitoring is designed for the Covid-19 suspected cases. In this regard it will inevitably reduce the over spread of that contagious virus. As described in the table below comparing the situation before and after our telemedicine platform:

	Before	after
Medical monitoring	Direct contact	Remote monitoring
High temperature detection	Direct measurement	Remote measurement
Temperature measurement	Each 30 minutes	In real-time
Statistical studies	At the end of the day	In real-time

Table 4: Country statistical board

date	New cases	Recovered cases	deaths	recovered rate	Recomm-endation
10/06/22	5000	3493	7	69%	Lock down
11/06/22	3000	2900	2	96%	Partial lockdown

5. Conclusion

In this paper all sides of the telemedicine were discussed to reduce as much as possible the over spread of Corona virus, primero starting by an overview of the digital solution, mentioning about the two parts; software and hardware. two advantages were highlighted, the real-time remote medical monitoring and the real-time statistics optimization as well.

In order to develop the POC (the proof of concept) of that solution, several didactic and academic items were. Such as the wireless shield for Arduino (NodeMcu) as a wearable network sensor node to acquire remotely the vital parameters of the suspected cases. For sure this last associated to the other sensors to enhance and confirm the feasibility of the project. Otherwise because of the covid situation there was no way to highlight the practical side of this research. In the same regard many interfaces were developed using LabVIEW, some of them are illustrated in this paper but others couldn't be inserted like the bloc diagram of the LabVIEW program. The next step of this research work is to move to the manufacturing process of the project including all the parts software and hardware.

6. References

[1] G. N. Iyer, "On the Analysis of COVID19 - Novel Corona Viral Disease Pandemic Spread Data Using Machine Learning Techniques," *4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2020.

[2] R. Caricchio, M. Gallucci, C. Dass, "Preliminary predictive criteria for COVID-19 cytokine storm", Annals of the Rheumatic Diseases vol. 80, pp. 88-95, 2021.

[3] V. Valerio, H.C. Shen, E. Field et. al., "POS1268 COVID-19 VACCINE HESITANCY AMONG RHEUMATOLOGY

PATIENTS RECEIVING INFLUENZA VACCINE", Annals of the Rheumatic Diseases, vol. 80, pp. 918-919, 2021.

[4] A. K. Tripathy, A. G. Mohapatra, S. P. Mohanty, E. Kougianos, A. M. Joshi and G. Das, "EasyBand: A Wearable for Safety-Aware Mobility during Pandemic Outbreak," *IEEE Consumer Electronics Magazine,* vol. 9, no. 5, pp. 57-61, 2020.

[5] C. H. Costin, A. Pasarica, I. Alexa, A. C. Ilie, C. Rotariu and D. Costin, "Short-term Heart Rate Variability using wrist-worn pulse wave monitor compared to a Holter ECG," *E-Health and Bioengineering Conference (EHB),* 2017.

[6] M. Protsiv, C. Ley, J. Lankester, T. Hastie, J. Parsonnet "Decreasing human body temperature in the United States since the Industrial Revolution," *eLife,* vol. 9, p. e49555, 2020.

[7] F. Margret Sharmila, P. Suryaganesh, M. Abishek and U. Benny "Iot Based Smart Window using Sensor Dht11," *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS),* pp. 782-784, 2019.

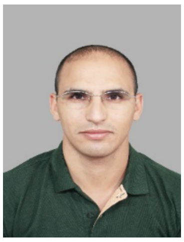
[8] P. Kaur and L. Mathew "Design and development of a graphical user interface for real time monitoring and analysis of vital human body parameters," *2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES),* pp. 1-8, 2016.

[9] D. Parida, A. Behera, J. K. Naik, S. Pattanaik and R. S. Nanda, "Real-time Environment Monitoring System using ESP8266 and ThingSpeak on Internet of Things Platform," *2019 International Conference on Intelligent Computing and Control Systems (ICCS),* pp. 225-229, 2019.

[10] M. Touil, L. Bahatti and A. Elmagri «Telemedicine application to reduce the spread of Covid-19,» *2020 IEEE 2nd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS),* pp. 1-4, 2020.

[11] G. Suprianto and Wirawan, "Implementation of Distributed Consensus Algorithms for Wireless Sensor Network Using NodeMCU ESP8266," *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS),* pp. 192-196, 2018.

[12] S. Gupta, G. Shankar, K. Kumari and S. Kumari,, "Load frequency control using BAT algorithm," *2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), Delhi, India,* 2016.



Mohamed TOUIL is a Ph.D. student at Hassan II University in Casablanca, High School of Technical Education (ENSET)-Mohammedia, Morocco, He received his Engineering Diploma in Biomedical Engineering from ENSAM-Rabat Mohammed V University of Rabat, Morocco on 2018. His current fields of study are Medical Images and Signals processing, Cardiovascular Implantable devices and wireless biosensors network (WSN) for medical telemonitoring. Mr. Mohamed TOUIL is a member of the research team Signal, Distributed Systems and Artificial Intelligence research center of ENSET Mohammedia. Morocco. Mr. Mohamed TOUIL has been dealing with medical systems for 4 years, as a Customer Service Engineer he worked with different companies. And for one year he is working with Siemens Healthineers as Customer Service Engineer.

Lhoussain BAHATTI is a teacher at Hassan II University in Casablanca, High School of Technical Education (ENSET)-Mohammedia, Morocco. He acquired his Ph.D. degree in Electrical Engineering Mohammed V University of Rabat, Morocco. He has published in the fields of electrical engineering and automatic and control, Renewable Energy Technologies and Kalman Filtering. Dr. Lhoussain BAHATTI is a member of the research team Distributed Systems and Artificial Intelligence research center of ENSET Mohammedia. Dr. Lhoussain BAHATTI he is occupying the position: Chief of Electrical Engineering department at ENSET Mohammedia, Hassan II university in Casablanca.

Abdelmounime ELMAGRI received his Ph.D. in Electrical Engineering – Automatic Control from Université de Mohammed V, Rabat, Morocco, in 2011. He is currently a professor at the Hassan II University, Casablanca Morocco. His research interests include optimization, observation and nonlinear control of AC machines and energy conversion systems.
He has coauthored several papers on these topics.

Special Issue on Multidisciplinary Sciences and Advanced Technology

Received: 14 April 2022, Revised: 29 June 2022, Accepted: 08 July 2022, Online: 27 July 2022

DOI: https://dx.doi.org/10.55708/js0107007

Research on Feature Extraction Method of Fiber Bragg Grating Vibration Monitoring Based on FFT

Mengxing Zhang, Youming Hua, Chunbin Chen, Chenkun Chu, Xiuli Zhang *

Faculty of Civil Engineering and Mechamnics, Jiangsu University, Zhenjiang, 212013, China
*Corresponding author: Xiuli Zhang, Jiangsu University, Zhenjiang, Email: 1000002674@ujs.edu.cn

ABSTRACT: Optical fiber is used in various fields because of its advantages of large-capacity communication, long-distance transmission, low signal crosstalk, good confidentiality, anti-electromagnetic interference, good transmission quality, small size, light weight, and long life. In this paper, the latest research progress of optical fiber sensing technology and its application and development in the field of rotating parts are summarized, and the characteristics and working principles of optical fiber intelligent composite materials are introduced. Fast Fourier Transform (FFT) and Hilbert fringe spectra are then applied to frequency component analysis. Quantitative research is carried out on the variation of the frequency components in each frequency band of the vibration signal of the damaged and non-damaged rotating parts. The method can analyze the fault signal to achieve the purpose of accurately extracting the fault characteristics of the rolling bearing, which plays an important guiding role in the accurate diagnosis of the bearing fault.

KEYWORDS: Fiber grating, Vibration monitoring, FFT, Feature extraction

1. Introduction

The acquisition and processing of fault signals is one of the main parts of fault diagnosis of rotating parts [1, 2]. When the rolling bearing fails, the frequency and amplitude of the fault signal will also change with time due to the influence of the type of fault, the degree of the fault and the change of the frequency of the rotating parts. Generally, the fault signal can be collected by fixing the fiber grating on the motor housing and collecting the vibration signal online [3-5]. In general, the fault diagnosis method of rotating parts is to obtain the actual frequency component of the signal through the processing and analysis of the fault signal, obtain the theoretical fault frequency of the signal according to precise calculation and analysis, and by comparing the two frequencies to further determine the type of rolling fault [6, 7]. However, when the rotating part fails, the analysis of the fault signal will find that the signal is often affected by the environment and the vibration of other parts of the rotating part, resulting in weak fault characteristics and easy to be overwhelmed by many noises [8]. Therefore, it has always been the research direction of domestic and foreign experts which method and means to use to analyze the fault problem of rotating parts, and effectively extract the fault features to realize the fault diagnosis of rotating parts.

Based on the above background analysis, this experiment aims to accurately extract the fault characteristics of the rotating parts, combined with the complex industrial environment and fault signal characteristics, comparing the signal perception and transmission efficiency of two types of acoustic emission sensors, and use the FFT frequency domain analysis method to analyze the fault signal to achieve the purpose of accurately extracting the fault characteristics of the rotating parts, it plays an important role in the accurate diagnosis of the fault of the rotating parts faults.

2. The mechanism of interaction between fiber Bragg gratings and acoustic emission waves

The fiber Bragg grating is closely attached to the surface of the object to be measured, as shown in Figure 1, the optical fiber material is used to make the sensitive structure of the rotating part, and the optical fiber directly embedded in the concrete structure. In this way, when the structure is deformed or otherwise defective due to changes in force and temperature, the gratings attached to the surface can deform, resulting in changes in the intensity, phase, wavelength and polarization of the light passing through the fiber. Based on the light variation information obtained, self-monitoring and diagnosis of stresses, deformations and cracks in rotating component structures can be determined [9, 10].

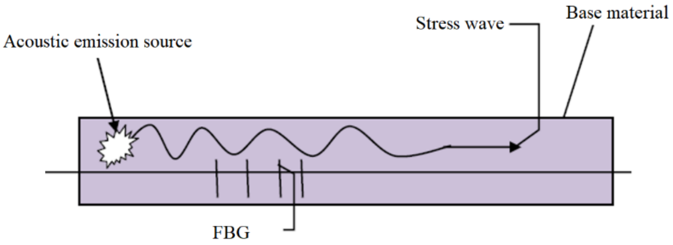


Figure 1: Fiber Bragg Gratings Interaction with Acoustic Emission Stress Waves

When the measured structure does not generate acoustic emission signals, the effective refractive index of the fiber Bragg grating is:

$$n_{eff}(z) = n_{ef0} - \Delta n\, sin^2\left(\frac{\pi}{\Lambda_0} z\right), z \in [0, L] \tag{1}$$

where, the length of the grating region is the amount of refractive index change. The strain field model generated by the surface acoustic emission stress wave is,

$$\varepsilon(t) = \varepsilon_m\, cos\left(\frac{2\pi}{\lambda_s} z - w_s t\right) \tag{2}$$

where ε_m is the stress wave amplitude generated by the acoustic source in the material, $2\pi/\lambda_s$ is the number of acoustic emission waves in a single acoustic emission event, ω_s is the angular frequency of the stress wave generated by the acoustic source, which can be expressed as $\omega_s = 2\pi f_s$, where f_s is the frequency of the acoustic emission wave, and λ_s is the wavelength of the stress wave generated by the acoustic source.

The variation of the central wavelength of the light emitted by the fiber grating is affected by both the period and the effective refractive index. Assuming that the fiber grating has a point z in the axial direction, it becomes z′ after modulation, and its relationship can be expressed by the following formula:

$$z' = f(z,t) = z + \int_0^z \varepsilon(\xi)d\xi = z + \varepsilon_m \frac{\lambda_B}{2\pi} sin\left(\frac{2\pi}{\lambda_s} z - w_s t\right) + \varepsilon_m \frac{\lambda_B}{2\pi} sin(w_s t) \tag{3}$$

where, $\int_0^z \varepsilon(\xi)d\xi$ is surface displacement due to acoustic emission waves.

Substitute $z' = f^{-1}(z,t)$ into equation (1),The change in refractive index n'_{eff}after modulation is calculated as,

$$n'_{eff}(z',t) = n_{eff0} - \Delta n\, sin^2\left(\frac{\pi}{\Lambda_0} f^{-1}(z',t)\right) \tag{4}$$

The effective refractive index of fiber grating can be expressed as,

$$\Delta n'_{eff}(z',t) = -\left(\frac{n^3_{eff0}}{2}\right) \cdot [P_{12} - v(P_{11} + P_{12})] \cdot \varepsilon_m\, cos\left(\frac{2\pi}{\lambda_s} z' - w_s t\right) \tag{5}$$

where p_{ij} is the elastic-optical coefficient of the fiber grating, and v is the Poisson's ratio of the fiber grating. The modulated fiber Bragg grating wavelength becomes,

$$\lambda_B(t) = \lambda_{B0} + \Delta\lambda_0\, cos(w_s t) \tag{6}$$

Among them, Δλ0 is the change in the amplitude of the center wavelength when it is affected by the acoustic emission wave.

$$\Delta\lambda_0 = \lambda_{B0}\varepsilon_m \left\{1 - \left(\frac{n^2_{eff0}}{2}\right) \cdot [P_{12} - v(P_{11} + P_{12})]\right\} \tag{7}$$

Under the condition of $\lambda_s/L \gg 1$, by detecting the change of the center wavelength of the reflected light of the fiber grating, the process of the continuous modulation of the fiber grating by the acoustic emission stress wave can be obtained.

Under the action of the acoustic emission signal of the fiber grating acoustic emission sensor, the center wavelength of the fiber grating in the fiber grating acoustic emission sensor changes, causing the reflected light to change. Through subsequent processing, the variation of the reflected light can be detected, and the corresponding acoustic emission signal can be obtained, so as to analyze the defects of the tested structure [11-14].

3. Grating experimental test device

Nine simulated pitting faults were evenly distributed by Empirical Mode Decomposition (EMD) on the outer ring of the rolling bearing. The load condition was 5kN, and the speed conditions were 600r/min and 1200r/min. When the bearing is running, the acoustic emission signal emitted by the collision between the fault point and other components is an instantaneous pulse signal, which has the characteristics of wide signal spectrum and rich low-frequency signal content. Install the resonant acoustic emission sensor, bare fiber grating, and encapsulated fiber grating sensor on the experimental platform. The placement of the acoustic emission sensor in the experiment is shown in Figure 2. Connect and debug the instrument. The fiber grating static demodulator is connected to the computer through the network cable, the IP address is set, and the demodulation software ENLIGHT is debugged to set the data storage path; the previously processed faulty bearing is placed on the bearing frame, the sensor is connected, and the bare fiber grating, The substrate-type fiber grating sensor is connected to the two channels of the SM125 static demodulator through the jumper, and the data is collected.

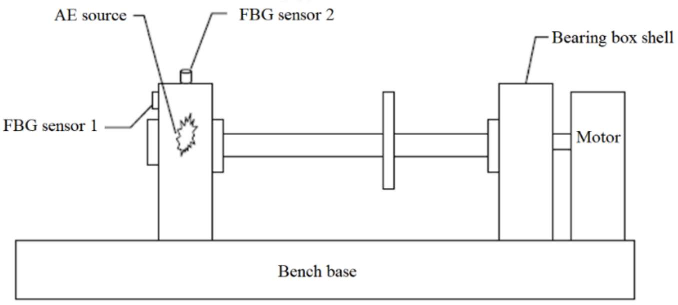
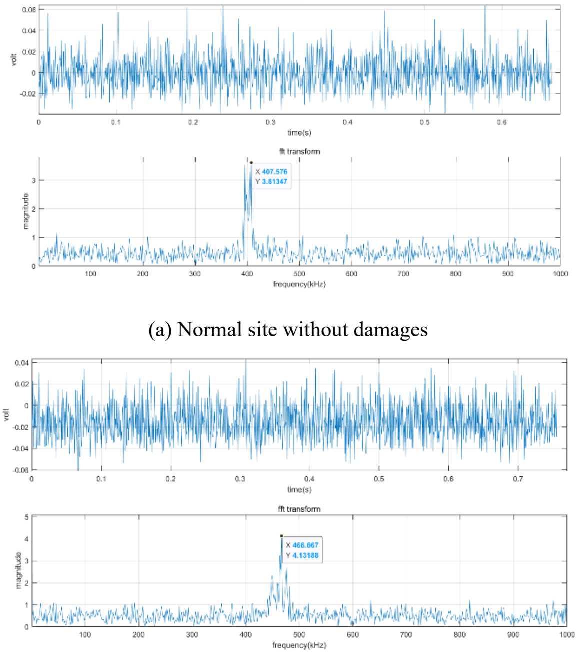


Figure 2: Experimental setup

4. Feature extraction of fiber grating vibration monitoring

Figure. 3 is the frequency spectrum obtained by FFT transformation of the signal measured by the rotating part involved in the experiment under the condition of rotating speed of 1400 revolutions/min. Figure 3(a) is the shell vibration signal of the fiber grating before the outer ring is damaged, and Figure 3(b) is the vibration signal after the inner ring is damaged. It can be seen that there is a difference in the main vibration frequency. The main vibration frequency of the spectrum obtained by FFT transformation They are 408kHz and 467kHz respectively. After many tests, it can be seen that the fiber grating sensor can correctly detect the existence of defects regardless of whether the crack is located on the surface of the outer ring, or inside the inner ring and rolling body.

The FFT transformation is performed using MATLAB software, which visualizes scientific data and models nonlinear dynamic systems.

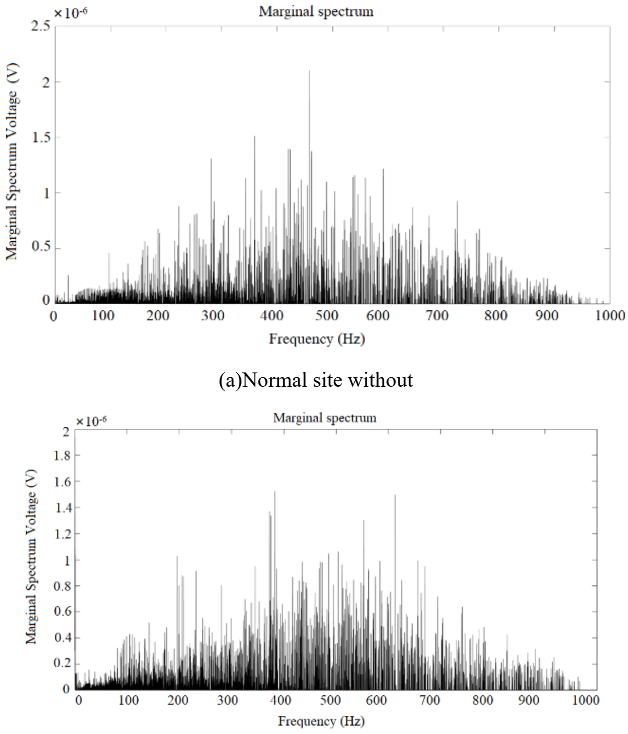


(a) Normal site without damages

(b) Crack damage in the inner bearing ring

Figure 3: FFT signal decomposition result

In order to quantitatively analyze the characteristics of elastic wave propagation during the rotational vibration of the rotating body, the marginal spectrum analysis of the fiber grating test signal is carried out. The traditional method is based on the fast Fourier transform (FFT) to obtain the frequency amplitude map. In this experiment, the Hilbert marginal spectrum is used to express the accumulation of the spectral amplitude at each frequency, which can more realistically reflect the frequency components. The amplitude has Additivity. Figure 4 shows the marginal spectral analysis results of the first-order IMF representing high-frequency components after different propagation distances. Under the condition of rotating speed of 1400 r/min, the Hilbert marginal spectral characteristic amplitudes of the vibration signals of the rotating parts before and after the destruction showed obvious differences. As shown in Figure. 4(a), the normal rotating parts show the characteristics of high relative change in amplitude in the low frequency range. While Figure. 4(b) shows the experimental rotating parts subjected to damage and damage treatment, the low frequency range below 200kHZ shows obvious characteristics of low relative change in amplitude, until the amplitude increases rapidly in the range of 200-300kHZ, showing high relative change in amplitude The characteristics of the FFT analysis were verified.



(a)Normal site without

(b) Crack damage in the inner bearing ring

Figure 4: Hilbert marginal spectrum under the rotating under 1400r/min

5. Conclusion

There are many new contents in the application of optical fiber sensing technology to the structure of rotating parts, and breakthroughs have been made in many key technologies, which have developed into a new branch with rich connotations, distinctive features and self-contained systems. In this paper, the vibration signal collected by the fiber grating is used to comprehensively analyze and study the frequency change of the vibration signal of the damaged and non-damaged rotating parts by FFT transformation, and it is concluded that it can be used for the health state monitoring of the rotating parts. The effectiveness of the FFT analysis method is verified by comparing the marginal spectral differences between the vibration signal processing results of the damaged and non-damaged rotating parts.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

This work was financially supported by the National Natural Science Foundation of China (11872191)

References

[1]. H. Shen, S. Li, D. Gu, et al., "Bearing defect inspection based on machine vision," Measurement, vol. 45, no. 4, pp. 719-733, 2012.

[2]. Q. Xiong, W. Zhang, Y. Xu, et al., "Diagnosing axle box bearings' fault using a refined phase difference correction method," Journal of Mechanical Science and Technology, vol. 33, no. 1, pp. 95-108, 2019.

[3]. J. D. Georgeson, "Inspection of Roller Bearing Surfaces with Laser Doppler Vibrometry," Journal of Manufacturing Science & Engineering, vol. 114, no. 1, pp. 123-125, 1992.

[4]. Y. T. Sheen, "A complex filter for vibration signal demodulation in bearing defect diagnosis," Journal of Sound & Vibration, vol. 276, no. 1-2, pp. 105-119, 2004.

[5]. Z. Fu, D. J. Brown, and B. P. Haynes, "A new method of non-stationary signal analysis for control motor bearing fault diagnosis," in IEEE International Symposium on Intelligent Signal Processing, 2003.

[6]. Z. Meng and S. S. Li, "Rolling bearing fault diagnosis based on improved wavelet threshold de-noising method and HHT," Journal of Vibration and Shock, vol. 32, no. 14, pp. 204-208+214, 2013.

[7]. J. Guo, X. Liu, S. Li, et al., "Bearing Intelligent Fault Diagnosis Based on Wavelet Transform and Convolutional Neural Network," Shock and Vibration, vol. 2020, no. 19, pp. 1-14, 2020.

[8]. G. Singh, R. Kumar, M. Singh, et al., "Detection of crack initiation in the ball bearing using FFT analysis," International Journal of Mechanical Engineering and Technology, vol. 8, no. 7, pp. 1376–1382, 2017.

[9]. G. Xuan, X.-P. Zhang, N. Ning, et al., "Research on Fiber Bragg Grating Acoustic Emission Technology Applied in Helicopter Bearing Detection," Procedia Engineering, vol. 99, pp. 1203-1212, 2015.

[10]. X. Zhou, H. Zhang, X. Hao, et al., "Investigation on thermal behavior and temperature distribution of bearing inner and outer rings," Tribology International, vol. 130, pp. 289-298, 2018.

[11]. L. Chen, Y. S. Choy, T. G. Wang, Y. K. Chiang, "Fault detection of the wheel in wheel/rail system using kurtosis beamforming method," Struct. Health Monitor. 19, no. 2, pp. 495-509, 2020.

[12]. X. Liu, D. Pei, G. Lodewijks, Z. Zhao, J. Mei, "Acoustic signal-based fault detection on belt conveyor idlers using machine learning," Adv. Powder Technol. 31, no. 7, pp. 2689-2698, 2020.

[13]. T. Tran, J. Lundgren, "Drill fault diagnosis based on the scalogram and melspectrogram of sound signals using artificial intelligence," IEEE Access, vol. 8, pp. 203655-203666, 2020.

[14]. L. A. L. Janssen, I. Lopez Arteaga, "Data processing and augmentation of acoustic array signals for fault detection with machine learning," J. Sound Vib., vol. 483, p. 115483, 2020.