*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7*
*DOI: https://doi.org/10.17762/ijritcc.v11i7.7826*
***Article Received**: 15 April 2023 **Revised**: 16 June 2023 **Accepted**: 30 June 2023*

# 9/7 LIFT Reconfigurable Architecture Implementation for Image Authentication

**Prakash Marakumbi[1], Satish Bhairannawar[2]**
[1]Department of Electronics and Communication Engineering
Tontadarya College of Engineering, Visvesveraya Technological University, Belagavi-590018
Karnataka, India
e-mail: pmarakumbi@gmail.com
[2]Department of Electronics and Communication Engineering
SDM College of Engineering & Technology, Visvesveraya Technological University, Belagavi-590018
Karnataka, India
e-mail: satishbhairannawar@gmail.com

**Abstract**— Considering the information system medical images are the most sensitive and critical types of data. Transferring medical images over the internet requires the use of authentication algorithms that are resistant to attacks. Another aspect is confidentiality for secure storage and transfer of medical images. The proposed study presents an embedding technique to improve the security of medical images. As a part of preprocessing that involves removing the high-frequency components, Gaussian filters are used. To get LL band features CDF9/7 wavelet is employed. In a similar way, for the cover image, the LL band features are obtained. In order to get the 1st level of encryption the technique of alpha blending is used. It combines the LL band features of the secret image and cover images whereas LH, HL, and HH bands are applied to Inverse CDF 9/7. The resulting encrypted image along with the key obtained through LH, HL, and HH bands is transferred. The produced key adds an extra layer of protection, and similarly, the receiver does the reverse action to acquire the original secret image. The PSNR acquired from the suggested technique is compared to PSNR obtained from existing techniques to validate the results. Performance is quantified in terms of PSNR. A Spartan 6 FPGA board is used to synthesize the complete architecture in order to compare hardware consumption.

**Keywords**- Teleradiology, Encryption, FPGA, PSNR, Medical Image

## I. INTRODUCTION

Teleradiology sends medical images through computer networks for clinical interpretation, improving access, delivery, and standards. Long-distance transmission of these images brings up a number of fresh and challenging legal and ethical questions, including those relating to image preservation and fraud, privacy, liability, and other security precautions in remote radiography. The factors are still in play. Digital medical picture distribution through networks has become essential to the functioning of the healthcare system on a regular basis. The main causes of this occurrence are two. The first is that compared to conventional film-based methods, digital imaging offers greater instruments for diagnosis, therapy, and surgery. The transfer of medical data across the network is crucial since the locations of medical examinations, where digital medical images are captured, and where those images are stored are frequently geographically apart. Due to the rapidly expanding trend in the healthcare sector that promotes sharing of digital medical images in order to better utilize resources there is an increased demand for the dissemination of digital medical images via public networks.

The current healthcare industry, including medical imaging facilities, hospital information systems (HIS), and hospital information management systems (HIMS), has been significantly impacted by recent technological advancements. Radiology medical imaging facilities are now more dependable and cost-effective, and film-based imaging processes are now filmless, producing digital images on a number of devices rather than physical copies. Using sophisticated radiological information systems (RIS), picture archiving and communication systems (PACS), and radiological information systems, use [1] these digitized medical images to assist hospitals in providing a variety of e-health services. These e-health services bring new processes for both professionals and patients by allowing remote access to, transfer of, and analysis of medical pictures for diagnostic reasons. This will promote the development of remote radiology, and improve healthcare delivery, access, and standards while raising potentially complex new ethical and legal problems. These difficulties include fraud, picture retention, PACS, RIS, and teleradiology contracts, as well as privacy, malpractice, and liability concerns. Radiology now places a high priority on security and privacy protection in teleradiology, one of the most effective e-health services available today. For a very long time, teleradiology was defined as an electronic health service that involved the analysis of supplied images for diagnostic purposes as well as the remote delivery of radiology images and data through electronic networks. Imaging is used in teleradiology to both identify and cure diseases that may be visible within the human body.

The definition of teleradiology as an electronic health service that involves the remote transmission of radiology pictures and data through electronic networks and the interpretation of the provided images for diagnostic purposes has been around for quite some time. Teleradiology uses imaging to find and treat disorders that can be seen inside the human body. Radiology pictures and information must be safeguarded with integrity, confidentiality, and appropriate administration by various healthcare services offering the necessary care. Remote access and transmission of radiology pictures and other data, especially [2] Electronic Personal Health Information(EPHI), exposes them to the risk of being altered or stolen, which could have detrimental effects. a set of security procedures that guarantee the profile's security ideas are followed, as well as a common set of privacy and security rules for teleradiology. Several national and international regulatory laws and standards outline the security and data protection requirements for medical information. Numerous established techniques are thought to be able to meet these requirements and provide the essential security of electronic radiation information with wireless PACS/RIS-based technology. On the other hand, current research suggests that the introduction of digital watermarks may improve the security of remote radiography. Watermarks [2] offer a variety of attractive properties that can enhance the security of various multimedia applications in addition to current security methods. When deciding if watermarks are acceptable for other comparable measures and whether they apply to all elements of the radiological information requirement, there are a few important factors to take into account.

## II. LITERATURE SURVEY

Information on image steganography with improved security is provided by the authors in [3]. The message is encrypted with an asymmetric version of the cipher text using the RSA encryption technique for increased security. The opposite is also accurate. The sender uses a key to encrypt the message, inserts the cipher text into the image, then sends the image object and key across a transmission medium, like the Internet, to the recipient. As a result, the recipient is able to separate the cipher text from the image and decrypt it using the sender's key. Although the results were only available in greyscale, they were satisfactory and met their purpose.

A safe system based on Android dubbed Steg has been proposed by Lalit Negi et al. [4]. It was created by fusing steganography and encryption. Advanced Encryption Standard (AES) is the encryption algorithm employed in this case, and steganography is performed using the least significant bit. By encrypting messages and disguising them as graphics, this hybrid strategy strengthens the secrecy of information and protects it from unauthorized access. With the use of this application, users can overlay text on photos. The above-mentioned system has been shown to be more effective and reliable than a system that only uses steganography and encryption.

An article using two distinct strategies was proposed by Srushti S. Yadahalli et al. [5], the discrete wavelet transform method and the least significant bit method, which both use the least significant bit of the cover image to conceal the secret image. The surreptitiously sent image is both encoded and decoded using these techniques and the resulting image is then thoroughly analyzed using a variety of image attributes. Therefore, the efficiency of the methodology suggested in the publication is indicated by these experimentally acquired and compared efficiency characteristics.

For the purpose of creating safe image encryption approaches for the healthcare sector, the authors of [6] offer an effective and portable encryption algorithm. The recommended lightweight encryption approach for protecting medical images uses two sequential steps. The security and execution speed of the suggested method is examined, evaluated, and compared with those of alternative well-known encryption techniques. The performance of the proposed method was evaluated on a large number of test photos. The results of the studies show that the algorithm of picture cryptosystems is more efficient than more conventional ones.

For constructing a GAN-based multi-step feature fusion approach, Zhen Wang et al. [7] developed an article more precise picture steganography method. The network is first given convolution and pooling procedures for feature extraction. The information about the multi-level feature is then combined using a short connection. Finally, conflict learning between the discriminator and the generator produces the Stego picture. According to experimental findings, the suggested technique has a higher ridge analysis safety in detecting ridge analysis with higher dimensional features and neural network ridge analysis.

The main areas of research in this work are the confidentiality and integrity of medical images [8]. Encryption can generally be used to achieve integrity and confidentiality. Medical image steganography is used to offer an extra layer of protection. In order to construct a steganography image, this technique first encrypts a medical image with a one-time pad encryption algorithm before embedding the encrypted image in a cover image, improving the system's resistance to an attacker. The technique also employs experimental findings to obfuscate medical photos with unencrypted LSB steganography. To compare, medical images in various formats, including DICOM, TIFF, BMP, and JPEG, are being taken into consideration. The outcomes demonstrate that the combination of encryption and steganography is superior to steganography alone in terms of MSE and PSNR scores.

To safeguard medical data, Muhammad Arslan Usman et al. [9] proposed a new imaging steganography method. The payload is losslessly compressed, put through a variety of encryptions, and then used with the swapped Huffman tree encoding in the cover image. Moreover, a significant degree of imperceptibility is offered by simply embedding secret data in the area surrounding the cover image. The findings demonstrate that the suggested method preserves imperceptibility while protecting patient data privacy and confidentiality.

The introduction of secure, interference-free medical data transfer is the primary driving force behind the study [10]. The image contains medical data because it is a different channel. This work includes creating a reliable, secure, and validated technique for sending a receiver private medical image from the sender. Sensitive portions of an image that are safe in inconspicuous pixel places are encrypted as part of the processes used to deliver images. Attempts to attack photographs must be discovered. Additionally, the original data must be very likely to be restored so that, in the event of an assault, medical photos are accessible. To achieve the desired encryption and recovery, the method leverages seed one-time pads.

A cryptographic system featuring a novel cryptographic technique, lossless compression technology, was proposed by Prema T. Akkasaligar et al. [12]. Lossless discrete medical image security is enhanced via chaos-based DNA encryption. The Haar wavelet transform is used to decrease the transmission's space and time efficiency. The suggested cryptosystem is secure against a variety of threats, according to cryptanalysis. To confirm that the stored medical image is similar to the original, pixel comparison is done with the compression ratio.

A new method of chaos-based medical picture encryption was put out by Mohamed A. in and others [13]. To avoid the potential of losing medical data during the encryption-decryption process, this technology employs a Butterworth First High-Pass filter that emphasizes the subtleties of medical images. In Arnold's cat card technique, the Advanced Encryption Standard (AES) algorithm is modified to change the three bits that Arnold's cat mapping technique adds to the usual AES encryption key. The technique was developed to improve encryption's overall robustness.

A new approach to encrypting and decrypting medical images based on deep learning networks is introduced in the work [14]. In order to transfer medical images from the source domain to the target domain, which is believed to contain a hidden factor, the first learning network, Cycle-GAN, was utilized. To achieve picture decoding, the encrypted image will be pieced back together as the original image using a reconstructed network. Data mining from privacy contexts is made easier by the Area of Interest (ROI) Mining Network, which was built to retrieve pertinent information from encrypted objects. The chest X-ray record is used to evaluate the suggested Deep EDN. The studies' findings demonstrate that the suggested method is effective and offers a higher level of security.

Sara T. Kamal et al. [15] proposed a new encryption method for encrypting grayscale and color medical images using segmentation technology on picture blocks. To jumble up the visuals, image blocks were subjected to random rotations, permutations, and zigzag patterns. The chaotic logistic map is then used to generate the key needed to send the encrypted image. The suggested method for encrypting medical images is evaluated in terms of time complexity and security. Histogram, differential attack, entropy, PSNR, correlation coefficient, keyspace, and sensitivity are used to test security. The outcomes show the high level of security attained by effectively encrypting medical photos in both grey and color. The suggested encryption algorithm outperforms current techniques for encrypting medical photos.

Reversible watermarks and robustness with three levels of security are offered in the work suggested in [16]. The region of interest and the interest-free area are the two divisions made by the algorithm for splitting up medical images. First, the payload data is reversibly embedded in a binary image in the region of interest. Therefore, when watermarking, changes are not made to the region of interest image. The use of strong watermarking is therefore implemented in interest-free zones in order to withstand both intentional and unintended attacks. Then, a watermark is inserted into the HL1 and LH1 subbands after using the Haar wavelet to create a two-level decomposition. To create a single merged watermarked image, additional watermarked photos are linked. The generated image is then processed using the AES algorithm to render it incomprehensible and so provide a high level of security. To recover the original image, a second decryption procedure is carried out.

The authors of the paper [17] outline a game theory-based solution for innovative lossless medical photo encryption that has optimized ROI settings and a hidden ROI position. The ROI is changed at the pixel level during the encryption process in order to achieve lossless decoding of the images and guard against losing the medical imaging data. This efficiently conceals the position of the ROI and prevents transmission-related position information leaking. A chaotic quantum cell neural network random sequence is employed to further dilute and muddle the ROI. The numerical outcomes demonstrate that the approach accomplishes lossless and perfect picture encryption and decryption while safeguarding various medical image sorts from numerous attacks.

An efficient chaos-based encryption technique for medical images was published by P. Sarosh et al. [18]. The method employs a Chebyshev map, a Piecewise Linear Chaotic Map (PWLCM), and a Logistic map to lessen confusion and dilute the medical image. Bit plane slicing is done after the image has been rotated in a circle. The Most Significant Bit (MSB) plane is then replaced by a plane made by conducting an XOR operation on the 7th ISB plane and the MSB plane. The image is then hidden by a pseudo-random number (PRN) generated by the logistic map. The parameter being tracked is regarded as mean since it creates the initial conditions for the PWLCM chaotic map, which is used to generate a key image. Then, an XOR operation is performed using the key image and the scrambled picture. To permute the image pixels and produce the final encrypted image, a PRN sequence is made, and then a Chebyshev map is iterated. This technique requires an average encryption time of 0.3287 seconds for a 256x256-pixel picture. The correlation coefficient for the images is virtually zero, and more than 99.70% of the entropy was obtained.

The authors of the study [19] suggest a novel chaos-based encryption method. It is built in two rounds using a combination of DNA computing and chaos theory. The initial secret keys and the SHA-256 hash algorithm are used to deduce the secret keys of the chaotic systems. Each cycle consists of six distinct operations: bit-level diffusion, block-based permutation, DNA encoding, and bit-level substitution. The logistic-Chebyshev map for bit-level substitution and the sine-Chebyshev map for bit-level diffusion are both used to construct key streams. To retrieve the encrypted image, the procedure is then carried out once more with the new keys. The technique is suitable for real-time picture applications and resilient to several low-complexity assaults, according to the result analysis.

A chaotic dynamic technique was described by V.Vanitha et al. [20] for synchronizing two chaotic systems and controllers. By combining the chaotic sequence with the disturbance term associated with the plaintext, the picture is created in this way. The cipher text feedback device for the dynamic index is then employed at the dissemination step. A secret key is created using complex logic after image encryption. Results of key sensitivity, differential analysis, key space analysis, entropy information, histogram, and correlation coefficient are used to demonstrate the efficacy and security of the suggested method.

In [21], the authors described a non-chaotic technique for image encryption. The Regula-Falsi method is used to substitute the pixel value and repeatedly add it with a cyclic shift to construct the encryption of an image. The outcome evaluations show that the method provides protection against a variety of attacks.

A novel method for digital image encryption is presented by Yousif, S.F., et al. [22] and is based on chaotic systems, bit replacement methods, and a DNA coding algorithm. The work focuses on safeguarding the secrecy and privacy of digital photo exchanges across open, unprotected networks that are susceptible to hacking. It starts by converting each visual pixel to its corresponding binary sequence of ones and zeros. The 1 bit is changed to (0 and 1) bits in the following stage, and the 0 bit is changed to (1 and 0) bits. The two distinct images are created by continually applying this procedure to all the bits. The positions and values of the digital image pixels are altered after the images created in the previous step using high-dimensional chaotic systems and diffusion processes. After being encoded using DNA algorithm principles in the third stage, the pictures are combined using a DNA addition operation. The encrypted image is produced following the decryption of the coded DNA images. The recommended approach passed all security and randomness checks, provided a substantial amount of secret key space (2747), equivalent differential analysis performance NPCR (99.61%), and UACI (34.61%), and passed all security and randomization tests.

The suggested work in [23] mentions a method of image encryption that focuses on the use of adaptable DNA code bases and new multi-chaotic map architecture. DNA coding improves data transmission and increases computer speed. The Gaussian, Henon, and Logistic (HGL) maps were combined to form the new multi-chaotic map, which results in more erratic pseudo-random sequences. Many analyses, including statistical, brute force, differential assaults, and noise addition studies, were done to demonstrate the excellent level of security that this system offers.

## III. PROPOSED METHOD

The method proposed uses CDF 9/7 and Alpha blending to embed the secret image information which is depicted in Figure 1.To remove any noise present both the secret data and the input cover image are pre-processed in parallel and then applied to Lifting DWT of CDF 9/7 to obtain the features of LL band. To achieve high speed and exploit parallelism the

CDF 9/7 and blocks of preprocessing are considered in parallel for both secret image and cover image. Further, both the LL band features that are obtained from CDF9/7 blocks are added to merge according to the technique of Alpha blending. The result of this technique with high-frequency components of LH, HL, and HH is then applied to inverse CDF 9/7 to get the embedded information and to transfer it over the channel [11]. Lastly, at the receiver end to decrypt the secret information the reverse process of encryption is carried out.

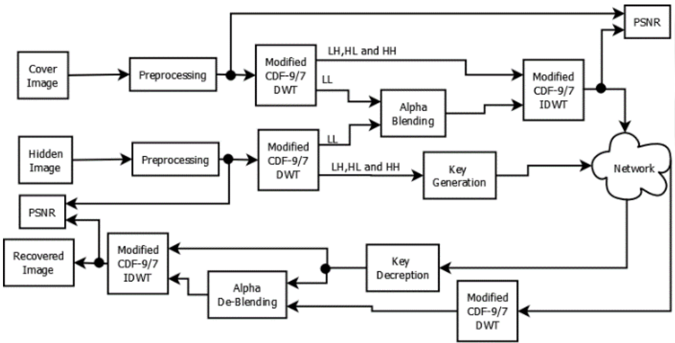

Figure 1. Proposed Block Diagram

### *A. Preprocessing*

The preprocessing includes the filtering of images with a Gaussian filter to remove the high-frequency components retaining the information. The basic purpose of a Gaussian filter is to eliminate random noise from images. Using moving window architecture, the 2nd-order Gaussian filter mask [23] coefficients of a 3x3 window are convolved with the sub-image of 3x3 pixels which is shifted throughout the image. The basic purpose of a Gaussian filter is to eliminate random noise from any image.

### *B.Gaussian Filter*

The filter is used to smoothen the image by removing high-frequency edges. The two-dimensional Gaussian filter [24] is given in (1).

$$g(x,y)=\frac{1}{2\pi\sigma^2}e^{-\frac{x^2+y^2}{2\sigma^2}} \qquad (1)$$

Where x is the distance in the horizontal axis from the origin

y is the distance in the vertical axis from the origin

σ denotes the standard deviation of the Gaussian distribution.

The 3x3 Gaussian mask filter is derived from (1) to obtain the mask [23] shown in (2).

$$Gaussian\ Mask=\frac{1}{16}\begin{bmatrix}1&2&1\\2&4&2\\1&2&1\end{bmatrix} \qquad (2)$$

Then the Gaussian filter is given in (3) by multiplying the 3x3 sub-matrix of an image with Gaussian mask.

$$Gaussian\ Filter=\frac{1}{16}\begin{bmatrix}1&2&1\\2&4&2\\1&2&1\end{bmatrix}*\begin{bmatrix}a_{33}&a_{32}&a_{31}\\a_{23}&a_{22}&a_{21}\\a_{13}&a_{12}&a_{11}\end{bmatrix} \qquad (3)$$

Where, $a_{11}$ to $a_{33}$ are 3x3 sub-matrix pixel values of an image.

$$Gaussian\ Filter=\frac{1}{16}[(a_{33}+2a_{32}+a_{31})+(2a_{23}+4a_{22}+2a_{21})+(a_{13}+2a_{12}+a_{11})]$$

$$Gaussian\ Filter=\frac{1}{16}[(a_{33}+a_{31}+a_{13}+a_{11})+2(a_{32}+a_{23}+a_{21}+a_{12})+4a_{22}]$$

$$Gaussian\ Filter=\frac{1}{2^4}[(a_{33}+a_{31}+a_{13}+a_{11})+2^1(a_{32}+a_{23}+a_{21}+a_{12})+2^2a_{22}]$$

$$Gaussian\ Filter=\frac{1}{(\gg 4)}[(a_{33}+a_{31}+a_{13}+a_{11})+(\ll 1)(a_{32}+a_{23}+a_{21}+a_{12})+(\ll 2)a_{22}] \qquad (4)$$

The proposed hardware structure for the Gaussian filter using(4) is shown in Figure 2.

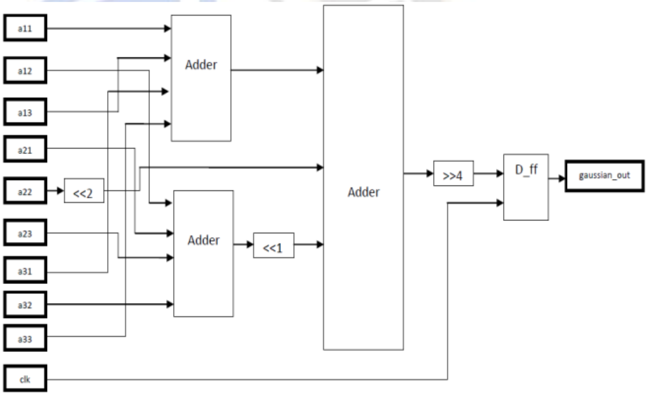

Figure 2. Gaussian filter Architecture

### *C. DWT and IDWT*

Considering an input signal x(i) the low pass(low(i)) and high pass(high(i)) outputs of this filter are obtained by convolution of x(i) with $h_0(i)$ and $h_1(i)$ respectively.

$$low(i)=\sum_{k=-4}^{4}h_0(k).x(i-k) \qquad (5)$$

$$high(i)=\sum_{k=-3}^{3}h_1(k).x(i-k) \qquad (6)$$

From Tables I, II & III substitute the values of filter coefficients and factorize our 9/7 filter coefficients in terms of 5/3 filter outputs

$$low_{9,7}(i)=low_{5,3}(i)-\frac{1}{32}W_0+\frac{1}{64}W_4 \qquad (7)$$

$$high_{9,7}(i)=\frac{1}{2}high_{5,3}(i)-\frac{1}{32}W_1+\frac{1}{32}W_3 \qquad (8)$$

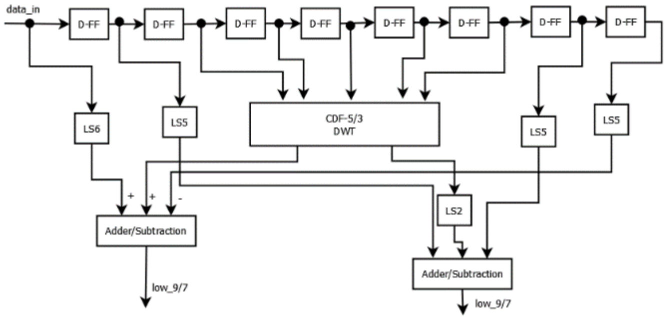

Figure 3. 9/7 Lift Architecture

*D. Alpha Blending and De-blending*

The secret images and LL band of the cover image are merged using Alpha blending technique [24]. The Alpha blending (9) is written as:

$$Watermarked\ Image = (1-\alpha)LL_{cover} + \alpha LL_{secret} \qquad (9)$$

Where, α is a constant value that varies from 0 to 1

$LL_{Cover}$ is the LL band coefficients of the cover image

$LL_{Secret}$ is the LL band coefficients of the secret image

Figure 4 shows the hardware architecture of the Alpha Blending technique. To get the optimized hardware utilizations efficient Koggy-Stone Adder/Subtractor [25] and Vedic multiplier [26] are used. To synchronize the watermarked data with the clk signal the D Flip Flop (DFF) is used.

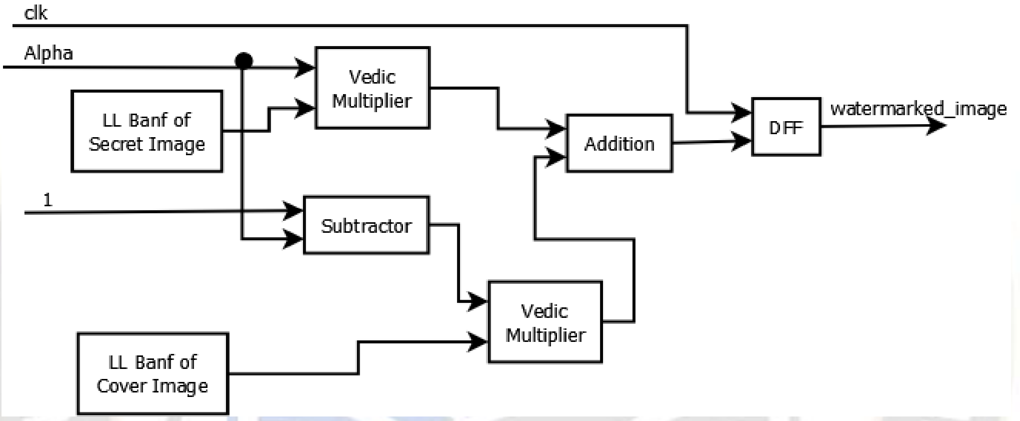

Figure 4. Alpha Blending Architecture using Vedic multiplier Koggy-Stone Adder/Subtractor

Similarly, from the standard [24] the optimized Alpha Deblending architecture is designed.

*E. Key Generation*

The LL, LH, HL and HH coefficient blocks are used to generate the dynamic key used for the encryption using matrix based encryption [29] technique which increase the security. The key generation equation is given in (10) where simple concatenation operation is used.

$$key = Y_{LH} \oplus Y_{HL} \oplus Y_{HH} \qquad (10)$$

## IV. RESULTS AND DISCUSSIONS

The proposed architecture is implemented on Digilent ATLYS FPGA [24] using System Generator tool where the standard VHDL language [28] is used for the coding purpose. The designed hardware model is shown in the Figure 5.

The Table I depicts the hardware utilizations of the proposed architecture It has 2171 slice registers or 2206 slice LUTs with 2695 LUT-FF pairs on Sparten-6 FPGA Board.

The simulation results of an X-ray image where the patient’s name and the date are embedded using the proposed steganography architecture is shown in the Figure 6 where it is possible to get maximum of 68.5 dB PSNR.

***Article Received**: 15 April 2023 **Revised**: 16 June 2023 **Accepted**: 30 June 2023*

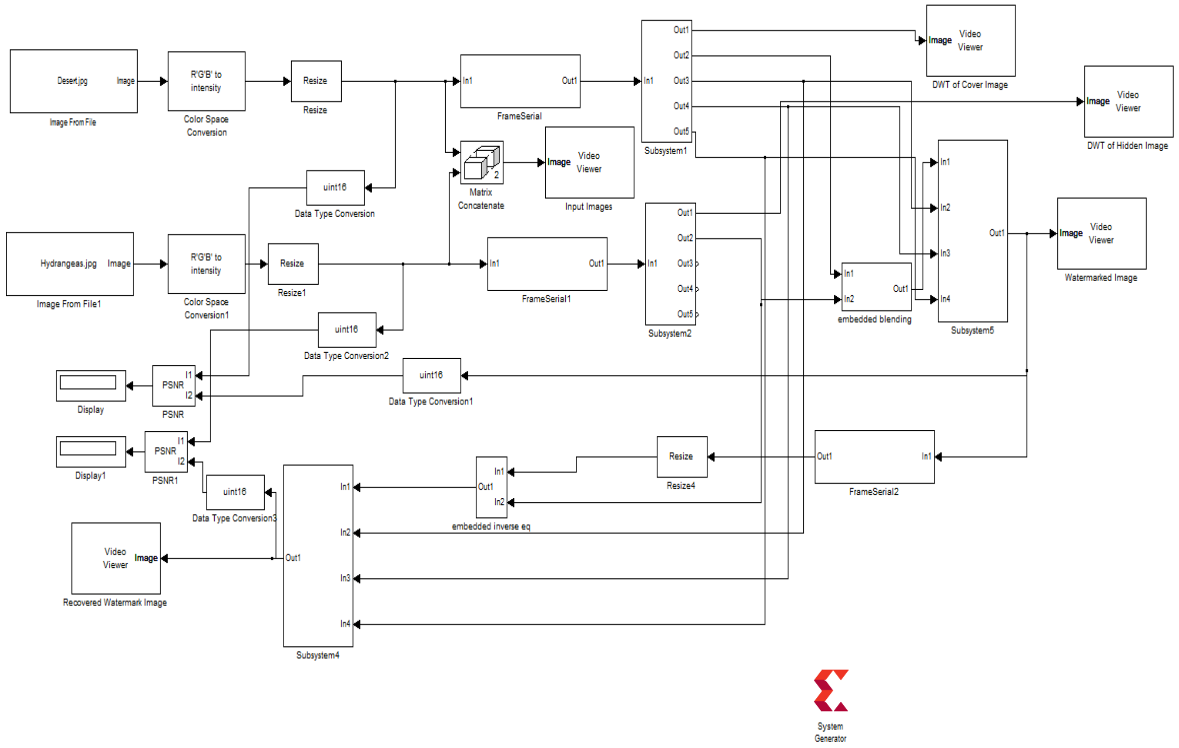

Figure 5. Design Model

TABLE I. HARDWARE UTILIZATION OF PROPOSED ARCHITECTURE

| Parameters | Hardware Utilizations |
|---|---|
| FPGA | Spartan-6 |
| Slice Registers | 2171 |
| Slice LUTs | 2206 |
| Memory | 32 |
| occupied Slices | 927 |
| LUT-FF | 2695 |

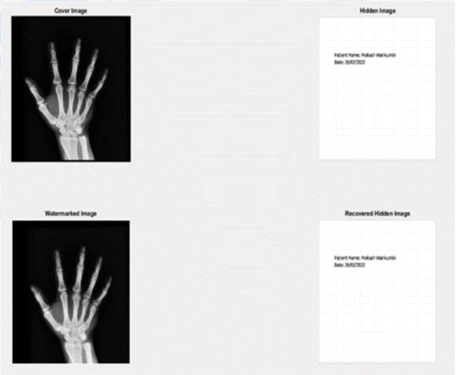

Figure 6. Simulation results

TABLE II. COMPARISON OF PSNR WITH EXISTING TECHNIQUES

| Authors | Techniques | Maximum PSNR (dB) |
|---|---|---|
| AyaJaradat et al., [29] | Chaotic particle swarm optimization | 69 |
| P. K. Muhuri et al., [30] | Integer wavelet transformation and particle swarm optimization | 52 |
| A. H. Mohsin et al.,[31] | Particle swarm optimization algorithm | 58 |
| Proposed | DWT and Alpha Blending algorithm | 68.5 |

From Table II it is observed that our method obtains maximum PSNR compared to the existing method as we have introduced a lossless CDF 7/3 Lift DWT with proper blended equation to combine the features followed by key generation. Table III shows that our slice registers and LUT-FF are better than the techniques presented by [32] and [33]. Since we use efficient koggy-Stone Adder/Subtractor [25] and Vedic multiplier [26] architectures to get optimized hardware utilization.

TABLE III. HARDWARE COMPARISON WITH EXISTING TECHNIQUES

| **Parameters** | **Nikhil Simha [32]** | **Jatin and Bhatt [33]** | **Hardware Utilizations** |
|---|---|---|---|
| FPGA | Spartan-6 | Nios- II processor | Spartan-6 |
| Slice Registers | --- | 2411 | 2171 |
| LUT-FF | 2108 | --- | 2695 |

## V. CONCLUSION

The necessity for medical image protection is not only to preserve confidentiality and handle confidentiality difficulties but also to prevent medical images from being modified by both authorized and unauthorized users. As a result, there is a way for maintaining data security, including medical imaging. In medical concepts, medical image encryption is a well-known method of ensuring data and picture confidentiality. In this paper, we offered a comprehensive and efficient medical image encryption technique. The encryption is tested for better PSNR values of medical images and also the hardware utilizations are compared to prove the efficiency.

## REFERENCES

[1] Maureen N. Hood, Hugh Scott," Introduction to Picture Archive and Communication Systems", Journal of Radiology Nursing, Volume 25, Issue 3, 2006, Pages 69-74, ISSN 1546-0843, doi:10.1016/j.jradnu.2006.06.003.

[2] Nyeem H, Boles W, Boyd C. "A review of medical image watermarking requirements for teleradiology". J Digital Imaging. 2013 Apr;26(2):326-43. doi: 10.1007/s10278-012-952 7-x.

[3] P. B, R. Harish, S. B and V. M, "Image Steganography using RSA Algorithm for Secure Communication," 2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC), 2021,pp.1-5,doi:10.1109/ ICM NWC52512.2021. 9688352.

[4] L. Negi and L. Negi, "Image Steganography Using Steg with AES and LSB," 2021 IEEE 7th International Conference on Computing, Engineering and Design (ICCED),2021,pp.1-6,doi: 10.1109/ICCED53389. 2021 .9664834.

[5] S.S.Yadahalli, S.Rege and R. Sonkusare, "Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques",5th International Conference on Communication and Electronics Systems (ICCES2020),pp.13251330,doi:10.1109/ICCES48766.2020.137 887 .

[6] Ravi, G. ., Das, M. S. ., & Karmakonda, K. . (2023). Energy Efficient Data Aggregation Scheme using Improved LEACH Algorithm for IoT Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 174 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2521

[7] M. K. Hasan et al., "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications", in IEEE Access, vol. 9, pp. 47731-47742, 2021, doi: 10.1109/ ACCESS. 2021. 3061710.

[8] Z. Wang, Z. Zhang and J. Jiang, "Multi-Feature Fusion based Image Steganography using GAN", 2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2021, pp. 280-281, doi: 10.1109/ ISSREW 53611. 2 021.00079.

[9] P.A, U. R, J. N and P. S, "Securing Medical Images using Encryption and LSB Steganography",2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), 2021, pp. 1-5, doi: 10.1109/ICAECT49130.2021.9392396.

[10] Prof. Deepanita Mondal. (2018). Analysis and Evaluation of MAC Operators for Fast Fourier Transformation. International Journal of New Practices in Management and Engineering, 7(01), 01 - 07. https://doi.org/10.17762/ijnpme.v7i01.62

[11] M. A. Usman and M. R. Usman, "Using image steganography for providing enhanced medical data security", 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018, pp. 1-4, doi: 10.1109/CCNC.2018.8319263.

[12] A. Srivastava, S. K. Awasthi, S. Javed, S. Gautam, N. Kishore and R. Bakthula, "Seeded One Time Pad for Security of Medical Images in Health Information", 2018 4th International Conference on Computing Communication and Atomation (ICCCA), 2018, pp. 1-6, doi: 10.1109/CCAA.2018.8777701.

[13] Rodríguez, M., Jovanović, A., Petrova, M., Merwe, M. van der, & Levi, S. Predicting Customer Lifetime Value with Regression Models. Kuwait Journal of Machine Learning, 1(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/144

[14] Prakash Marakumbi, Satish Bhairannawar "Efficient reconfigurable architecture to enhance medical image security", Indonesian Journal of Electrical Engineering and Computer Science Vol. 30, No. 3, June 2023, pp. 1516~1524 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v30.i3.pp1516-1524.

[15] P. T. Akkasaligar and S. Biradar, "Medical Image Compression and Encryption using Chaos based DNA Cryptography", 2020 IEEE Bangalore Humanitarian Technology Conference (B-HTC), 2020, pp. 1-5, doi: 10.1109/B-HTC509 70.2020.

[16] M. A. W. Shalaby, M. T. Saleh and H. N. Elmahdy, "Enhanced Arnold's Cat Map-AES Encryption Technique for Medical Images", 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES), 2020, pp. 288-295, doi: 10.1109/NILES50944.2020.9257876.

[17] Y. Ding et al., "DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things", in IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1504-1518, 1 Feb.1, 2021, doi: 10.1109/JIOT.2020.3012452.

[18] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images", in IEEE Access, vol. 9, pp. 37855-37865,2021, doi: 10.1109/ACCESS.2021. 3063237.

[19] A. Shankar and A. Kannammal, "A Hybrid Of Watermark Scheme With Encryption To Improve Security Of Medical Images", 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 226-233, doi: 10.1109/ICICV50876 .2021. 9388616.

[20] 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", in IEEE Access, vol. 8, pp. 122210-122228, 2020, doi: 10.1109/ACCESS .2020 .3007550.

[21] Renato Costa, Deep Reinforcement Learning for Autonomous Robotics , Machine Learning Applications Conference Proceedings, Vol 2 2022.

[22] P. Sarosh, S. A. Parah and G. Mohiuddin Bhat, "Fast Image Encryption Framework for Medical Images", 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 149-154, doi: 10.1109/ICIEM 51511.2021.9445362.

[23] A. Belazi, M. Talha, S. Kharbech and W. Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding", in IEEE Access, vol. 7, pp. 36667-36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[24] Vanitha, V., Akila, D." Bio-medical Image Encryption Using the Modified Chaotic Image Encryption Method", Lecture Notes in Computational Vision and Biomechanics, (2023)vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-01 51-5_20

[25] Paul, A., Kandar, S. & Dhara, B.C. "Image encryption using permutation generated by modified Regula-Falsi method". Appl Intell 52, 10979–10998 (2022). https://doi.org/10.1007/s10489-021-03063-1

[26] Yousif, S.F., Abboud, A.J. & Alhumaima, R.S. "A new image encryption based on bit replacing, chaos and DNA coding techniques", Multimed Tools Appl 81, 27453–27493 (2022). https://doi.org/10.1007/s11042-022-12762-x

[27] Ismail, R., Fattah, A., Saqr, H.M. et al. "An efficient medical image encryption scheme for (WBAN) based on adaptive DNA and modern multi chaotic map". Multimed Tools Appl (2022). https://doi.org/10.1007/s11042-022-13343-8

[28] Sayantam Sarkar and Satish S Bhairannawar, "Efficient FPGA Architecture of Optimized Haar Wavelet Transform for Image and Video Processing Applications", Journal of Multi dimensional Systems and Signal Processing, Springer, Vol. 32, pp. 821-844, April 2021 (DOI: 10.1007/s11045-020-00759-4).

[29] Anbumani V,Soviya S, Sneha S and Saran L, "Speed and Power Efficient Vedic Multiplier using Adders with MUX", IEEE Innovations in Power and Advanced Computing Technologies (i-PACT), pp. 1-5, 2021.DOI: 10.1109/i-PACT5 2 855.2021.9696992

[30] Datasheet of Digilent ATLYS FPGA board. [Online] Available at:https://reference.digilentinc.com/_media/atlys:atlys:atlys_ rm .pdf.

[31] Steven T. Karris. "Introduction to Simulink with Engineering Applications". Gatesmark Publishing, 2nd edition, 2006.

[32] Charls H. Roth (Jr.), "Digital System Design using VHDL", Cengage Learning, 2006.

[33] AyaJaradat, EyadTaqieddin and MoadMowafi, "A High-Capacity Image steganography Method Using Chaotic Particle Swarm Optimization", Security and Communication Networks, Hindawi, pp. 1-11, 2021.

[34] Qureshi, D. I. ., & Patil, M. S. S. . (2022). Secure Sensor Node-Based Fusion by Authentication Protocol Using Internet of Things and Rfid. Research Journal of Computer Systems and Engineering, 3(1), 48–55. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/41

[35] P. K. Muhuri, Z. Ashraf and S. Goel, "A novel image steganographic method based on integer wavelet transformation and particle swarm optimization," Applied Soft Computing, Elsevier, vol. 92, pp. 1-41, 2020.

[36] A.H. Mohsin, A. A. Zaidan, B. B. Zaidan and Salem Garfan "New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity," IEEE Access, vol. 7, pp. 168994–169010, 2019.

[37] Nikhil Simha H.N., Pradeep M. Prakash, Suraj S. Kashyap , Sayantam Sarkar "FPGA Implementation of Image Steganography Using Haar DWT and Modified LSB Techniques." IEEE International Conference on Advances in Computer Applications (ICACA), pp 26-31, 2016

[38] Jatin Chaudhari and K.R.Bhatt, "FPGA Implementation of Image Steganography: A Retrospective", International Journal of Engineering Development and Research, pp. 2117-2121, Volume 2, Issue 2, 2014.