Efficient reconfigurable architecture to enhance medical image security

Prakash Marakumbi[1], Satish Bhairannawar[2]
[1]Department of Electronics and Communication Engineering, Tontadarya College of Engineering, Gadag, India
[2]Department of Electronics and Communication Engineering, SDM College of Engineering, Dharwad, India

Article Info

Article history:

Received Nov 16, 2022
Revised Jan 31, 2023
Accepted Feb 4, 2023

Keywords:

Encryption
Field-programmable gate array
Medical image
Peak signal-to-noise ratio
Teleradiology

ABSTRACT

Medical images are one of the most critical and sensitive types of data in information systems. For the secure storage and transfer of medical images, confidentiality is the most important aspect. This paper presents efficient embedding technique to enhance medical image security. The Gaussian filters are used as preprocessing to remove high frequency components and then applied to cumulative distribution function (CDF) 5/3 wavelet to obtain LL band features. Similarly, the LL band features of cover image are obtained. The alpha bending technique combines both the LL band features of cover and secret image to form first level of encryption and now with other high frequency bands of LH, HL, and HH applied to Inverse CDF 5/3 obtains an encrypted image which is then transferred along with key obtained through other bands of LH, HL, and HH. The key generated acts as additional level of security and similarly, at the receiver the opposite operations are performed to obtain the original secrete image. The performance is measured in terms of Peak signal-to-noise ratio (PSNR) and is compared with existing techniques to validate the results. Further, the entire architecture is synthesized on spartan 6 field-programmable gate array (FPGA) board to compare the hardware utilizations.

Corresponding Author:

Prakash Marakumbi
Department of Electronics and Communication Engineering, Tontadarya College of Engineering
Gadag-582101, India
Email: pmarakumbi@gmail.com

1. INTRODUCTION

The internet has emerged as the primary communication medium for transmitting, disseminating, and exchanging data among users as a result of significant technological advancements and rapid expansion [1]. People may communicate knowledge quickly, easily, and affordably through the internet [2]. There is still a gap in terms of security and privacy. Two such qualities are sincerity and integrity [3]. Additionally, people are using the Internet more frequently as a primary form of communication [4].

On the other hand, one of the most important challenges in the globe is improved healthcare quality. The provision of healthcare to people is frequently seen as the most crucial issue on earth [5]. Public access to higher quality medical care is made possible by information technology. The practise of providing medical care to patients and doctors who are geographically apart via the use of information and communication technology is known as telemedicine. Digital medical information, such as medical images, are easily and quickly made available to the healthcare industry via contemporary health care systems like the hospital information system (HIS) and the picture archiving and communication system (PACS) [6]. In the field of telemedicine, the medical image is acknowledged as a key element. In hospitals, it is used for diagnostic purposes. As a result, every change in the patient's condition, no matter how little, will affect the physician's diagnosis. To ensure that only legitimate changes occur, medical images require a high level of security [7]. These days, medical image interchange across clinics in different geographic regions is rather common. Unfortunately, this communication takes place through insecure and open networks, increasing the possibility of malicious behavior and, as a result, data corruption or deletion [8]. Due to these restrictions and dangers, telemedicine necessitates secure interchange circumstances to safeguard the validity and integrity of medical pictures while they are being transmitted. Hospitals take a huge quantity of medical photographs, which are then saved in databases for analysis and diagnosis. These databases need to be secured against both deliberate and accidental attacks [9]. These databases make it possible to detect and cure diseases early. Before making a choice, the doctor must verify that the image has not been altered.

Digital medical image protection must have at least two essential features: security and authenticity. Security requires the protection of data from unauthorised users, and authentication ensures that the data received hasn’t been tampered with or altered and that it came from the intended sender [10]. After the medical image has been transferred, confidentiality, authenticity, and reliability must all be guaranteed [11]. Unauthorized users are not permitted to view or access the medical image in any way, let alone edit it or draw any conclusions from it. The keyholder can access the patient data on the destination side by decrypting the encrypted medical image [12]. Watermarking techniques [13] were developed as additional data integrity, authenticity, and originality protection mechanisms. We can still tell if the data has been tampered with or is in its original state after decryption. Cryptography [14] plays an important role in this where the data can be decrypted in a usable format by someone who possesses the secret key and algorithm. The data, however, is no longer secure after decryption. As a result, determining its authenticity and origin is quite difficult. Priori protection measures are the name given to this type of security. One of our study goals is to secure and demonstrate the security of medical images [15]. This entails proving the medical image’s legitimacy as well as its integrity and originality.

2. LITERATURE SURVEY

Vaseghi *et al.* [16] developed a fast finite time synchronisation technique for chaotic systems that could be used for medical imaging encryption. The authors of this study first created an adaptive terminal sliding mode tracking method with quick reaching conditions, then they created a chaotic cryptosystem with a synced chaotic scheme serving as the secret key generator. The test results show that the suggested approach is dependable, usable, and has a high rate of convergence.

A lightweight encryption method has been suggested Hasan *et al.* [17] to enhance the security of medical picture data on applications for the internet of medical things. In this study, a safe image encryption approach for the healthcare sector is improved using an efficient, lightweight encryption technology. Two permutation approaches are used in the recommended light weight encryption system to safeguard medical photos. Trials show that the projected method is faster than traditional methods for generating medical images.

A deep learning-based stream cipher generator for medical image encryption and decryption was proposed Ding *et al.* [18]. To generate the private key, DeepKeyGen uses the generative adversarial network (GAN) as the learning network. The field of alteration has developed to the point where it can monitor the learning network and compile information on the creation of private keys. Trials demonstrate that the offered technology encrypts multimodality medical images successfully and effectively.

Han *et al.* [19] suggested a hermite chaotic neural network based medical image encryption algorithm. The logistic map’s initial chaotic sequence serves as the medical image encryption mechanism in the projected method. After training a Hermit chaotic neural network with the chaotic sequence, the medical image is subsequently encrypted using two key streams. Strong key compassion, efficient encryption and decoding, and statistical analysis conflict can all be seen in the proposed method.

Joint watermarking encryption JPEGLS is suggested Haddad *et al.* [20] for medical image reliability control in encrypted and compressed domains. The recommended solution has been praised for its ability to enable access to watermarking-based security features from both compressed and encrypted picture bit streams without even basic decryption. This is its main point of differentiation. Trials of the suggested technology demonstrate that it reliably transmits a message in both encrypted and compressed fields while minimising image distortion.

Khan *et al.* [21] proposed medical image encryption in smart healthcare IoT systems. This project aims to secure medical data via image encryption. The authors employ pixel adaptive dispersion theory and three rounds of high-speed knotting to suppress arbitrary neighbouring pixels. The experiment results show that the suggested approach has a high security standard for protecting the smart healthcare IoT system.

A deep learning-based image encryption and decryption network for the internet of medical things was presented Ding *et al.* [22]. The cycle generative adversarial network (Cycle GAN) is specifically employed as the fundamental learning network in DeepEDN to transfer the medical picture from its original field to the targeted field. According to the investigations, the suggested method can more successfully encrypt and decrypt the medical image while retaining a high security layer.

To encrypt certain medical photos, Akkasaligara and Biradar [23] suggested using deoxyribo nucleic acid (DNA) cryptography. This work employs dual hyperchaotic map methods and DNA cryptography to deliver high level security to medical imaging. Tests have been done to demonstrate that the suggested solution uses less processing time, making it appropriate for telemedicine, smart health, and e health applications.

Maurya *et al.* [24] have suggested an extended visual cryptography technique for medical image security. Secret information can be shared in visual, textual, and other media using visual cryptography. The suggested procedure inserts the medical image into three cover images after first encrypting it. Trials show that the encryption and insertion algorithms used in this process are lossless and simpler.

Kumar *et al.* [25] suggested a fractional discrete cosine transform with chaotic function for medical image encryption. This paper provides a brand-new technique for protecting medical data: applying a chaotic map to the coefficients of medical images' fractional discrete cosine transform (FrDCT). The chaotic map on FrDCT coefficients and applying FrDCT on the image are the two steps of the projected technique. The results of the trials show that the proposed strategy should be more closely related to other state of the art methodologies.

For the secure transmission of authenticated watermarked medical images, Priya and Santhi [26] suggested a novel visual medical image encryption technique. Basic picture encryption uses an unidentifiable, noise like image format to indicate the presence of secret data in the encrypted image. This study presents a groundbreaking technique for visual medical image encryption that ensures the presence of watermarked medical images to address this problem. Trials have shown that the suggested approach decreases the strain of the invader while still delivering a decent outcome.

Secure IoT solutions for medical image encryption were created Mishra and Acharyan [27] using high throughput and small area designs. The secure internet of things (SIT) algorithms utilised in reserve force applications are presented in this study as high speed and small area designs. In high frequency applications, the projected pipeline architecture is advantageous, whereas the projected sequential architecture is advantageous in low area environments. Trials on the suggested method show that it is faster and takes up less space, which lowers the cost of the gear.

Banu and Amirtharajan [28] suggested a chaos DNA integer wavelet transform (IWT) combo technique for medical image encryption in the dual domain. This paper suggests digital imaging and communications in medicine (DICOM) picture encryption. The proposed technique generates pseudo random encryption keys using a logistic map and a chaotic 3D lorenz attractor. The results demonstrate how robust the suggested approach is against brute force attacks.

A Latin square and memristive chaotic system-based approach for encrypting medical images has been proposed Chai *et al.* [29]. The permutation and diffusion architecture are used in the suggested method. A permutation based on latin square and plain image (PPILS) approach is suggested using Latin square and plain image data. The research has improved the security and sturdiness of picture encryption, which is relevant to applications for medical image encryption, according to testing results.

Dagadu *et al.* [30] suggested medical image encryption based on hybrid chaotic DNA diffusion. The suggested procedure consists of two steps: scattering DNA and producing a chaotic key. The message abstract method compares the plain image matrix to the two chaotic matrices row by row after applying five hash operations to a simple medical image. The proposed strategy is valid and challenges a number of epidemic methodologies, as demonstrated by the numerical, differential, and key analysis tests.

3. METHOD

The proposed method for embedding of secret image information using cumulative distribution function (CDF) 5/3 and alpha bending technique is as shown in Figure 1. The input cover image and the secret data image are both parallelly preprocessed for removal of any noise and then applied to lifting discrete wavelet transform (DWT) of CDF 5/3 to obtain the 2D LL band features. The blocks of preprocessing and CDF 9/7 are considered in parallel for both cover and secret image, which exploits the parallelism and achieve high speed. Now both the LL band features obtained from CDF 9/7 blocks are used to merge according to alpha blending technique. The output of alpha blending with high frequency components of LL, LH, and HL are applied to inverse CDF 9/7 to obtain the embedded information to be transferred over the channel. Finally, the secret information at the receiver end is decrypted by performing the reverse process of encryption.

3.1. Preprocessing

The images are filtered with Gaussian filter which removes the high frequency components retaining the information. The second order Gaussian filter mask coefficients of 3x3 window are convolved with the sub image 3x3 pixels shifted throughout the image using moving window architecture. Gaussian filter is mainly used to remove random noise present in any image.

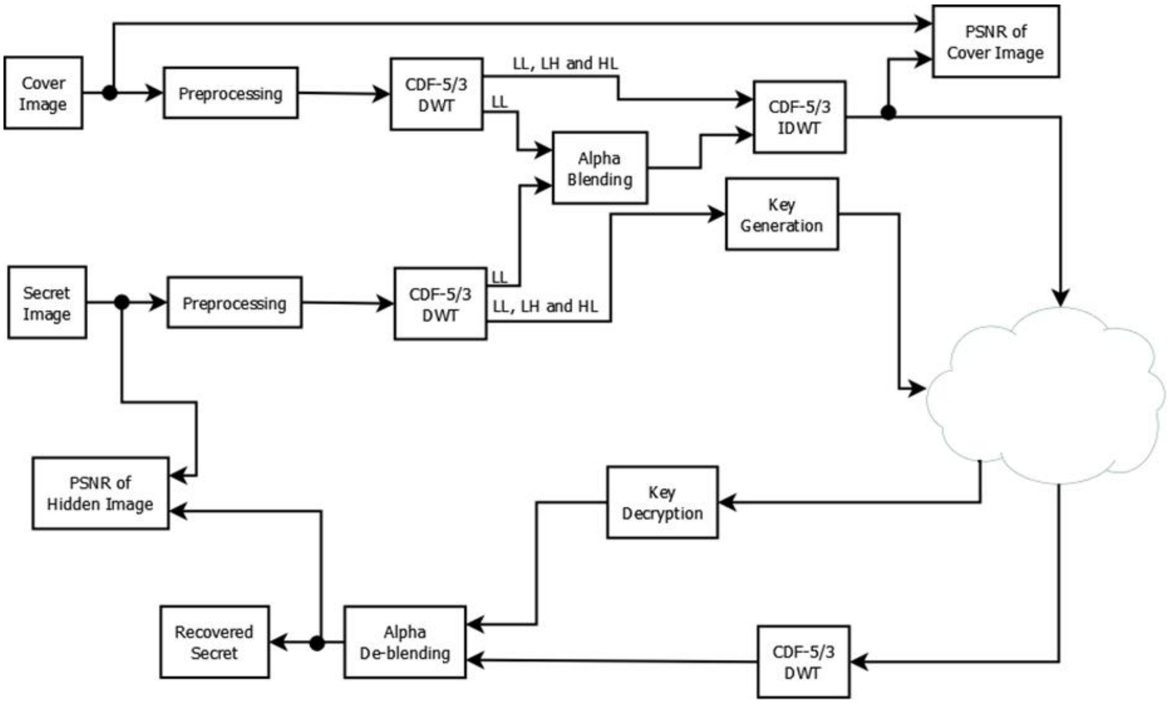

Figure 1. Proposed block diagram

3.2. Lift DWT and IDWT

The CDF lift DWT 5/3 is used for extracting the compressed features from image. The CDF 5/3 wavelet is lossless in nature. This wavelet is employed when signal accuracy is a concern because of this characteristic.

3.2.1. Mathematical formulation of lift DWT

The basic lifting schemes for CDF 5/3 [31] are given in (1) and (2). The (1) and (2) are simplified to get high pass and low pass filter coefficients. Table 1 represents the filter coefficients of 5/3 DWT.

$$y[2n+1] = x[2n+1] - \left[\frac{x[2n]+x[2n+2]}{2}\right] \quad (1)$$

$$y[2n] = x[2n] + [y[2n-1] + y[2n+1]] \quad (2)$$

Table 1. Filter coefficients of 5/3 DWT

i	LPF coefficient	HPF coefficient
0	3/4	1/2
±1	1/4	-1/4
±2	-1/8	0

3.2.2. Proposed 1D and 2D DWT architecture

The proposed 5/3 DWT is separable. The 2D DWT design can be split into two distinct 1D DWT blocks for the row processor and column processor. The proposed 1D and 2D DWT is described.

a. 1D DWT architecture

Figure 2 depicts the proposed 1D fundamental DWT’s block diagram. One multiplier, two add/shift units, one first ın first out (FIFO), six shifters, one multiplier, and one clock divider make up the entire 1D DWT block. Decimation blocks are often made using a clock divider. Four clock cycles constitute the delay of this 1D DWT block. An extra signal called rst out is used as the output port to communicate that the device is ready. Here, we employ a single counter that goes up to four and then stays constant. The rst out signal, which indicates that the 1D DWT block is ready to create the output, will be high when this counter reaches the count.

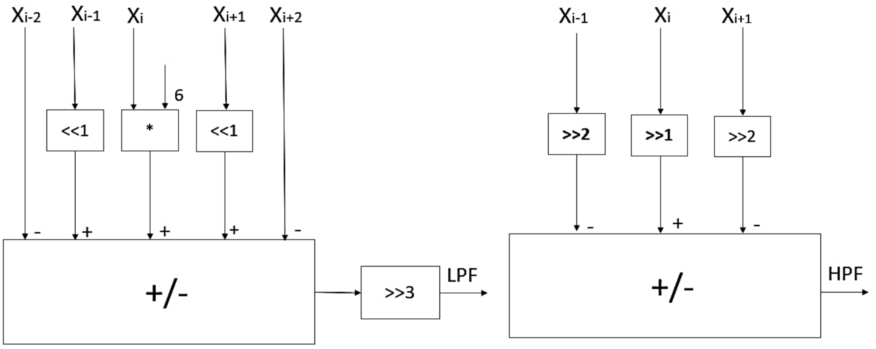

Figure 2. Proposed 1D DWT architecture

b. **Proposed 2D DWT architecture**

Figure 3 depicts the 2D fundamental DWT's block diagram. This module is made up of one DWT memory block and three 1D DWT's. To offer one level compression for input images, the 1D DWT block DWT0 converts 256×256 images into either 128×256 or 256×128 images depending on the input reading technique of the picture data. DWT memory contains the compressed picture pixel data. This memory block is utilised to get the transposed version of the compressed input image pixels. The LL, LH, HL, and HH bands are created by sending this transposed image to the DWT1 and DWT2 blocks. In the similar way the IDWT blocks are implemented.

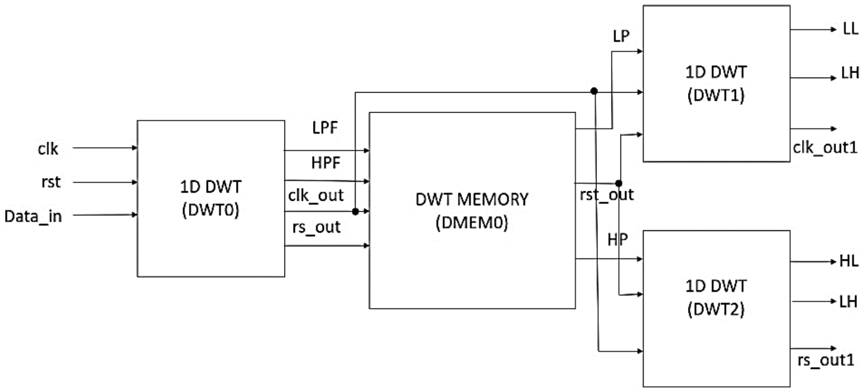

Figure 3. Proposed 2D DWT architecture

3.3. Alpha blending and De blending

The LL band of the cover and secret images are merged using alpha blending technique. The alpha blending [32] can be written as:

$$Watermarked\ image = (1 - \alpha) \times LL_{Cover} + \alpha \times LL_{Secret} \tag{3}$$

where, α is constant value varies from 0 to 1: $LL_{Cover}$is the LL band coefficients of the cover image and $LL_{Secret}$is the LL band coefficients of the secret image.

The hardware architecture of the alpha blending is shown in the Figure 4 where efficient koggy stone adder/subtractor [33] and vedic multiplier [34] architectures are used to get optimized hardware utilizations. The D FlipFlop (DFF) is used to synchronize the watermarked data with the clk signal. In the similar manner, the optimized alpha deblending architecture is designed from the standard [32].

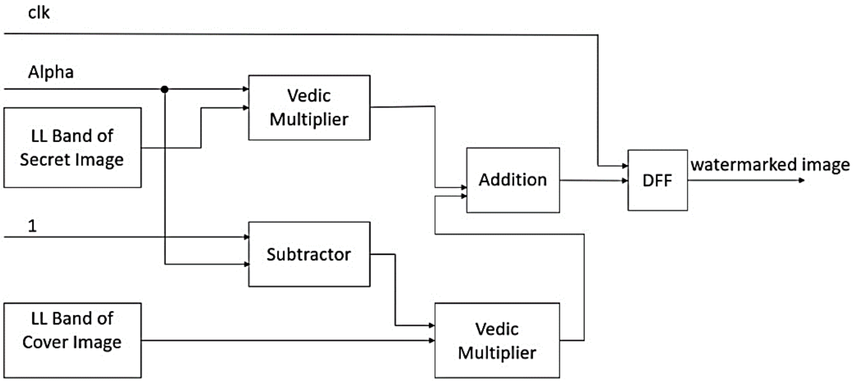

Figure 4. Hardware architecture of alpha blending

3.4. 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 [35] technique which increase the security. The key generation is given into (4) where simple concatenation operation is used.

$$key = Y_{LH}\ CONCAT\ Y_{HL}\ CONCAT\ Y_{HH} \tag{4}$$

4. RESULTS AND DISCUSSION

The proposed architecture is implemented on digilent Atlys FPGA [36] using system generator tool [37] where the standard VHDL language [38] is used for the coding purpose. The designed hardware model is shown in the Figure 5. The hardware utilizations of the proposed architecture is shown in Table 2 which utilizes 1,676 slice registers or 1,773 slice LUTs with 2,067 LUT FF pairs on sparten 6 FPGA board.

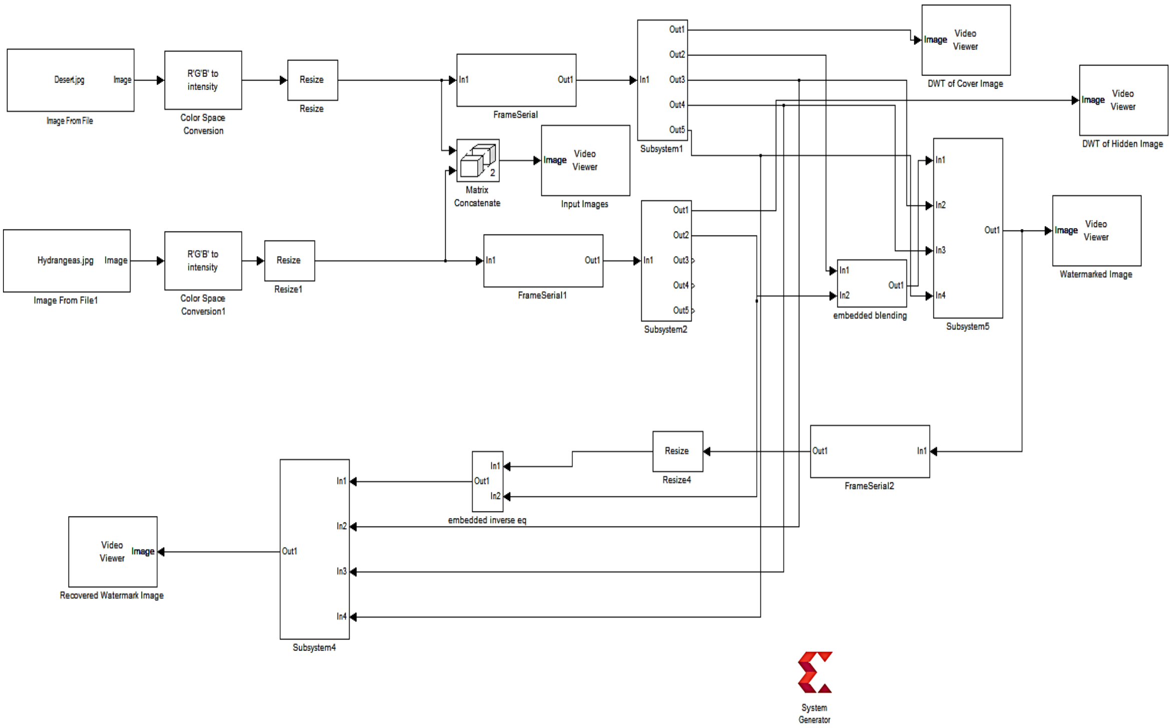

Figure 5. System generator model of the proposed architecture

Table 2. Hardware utilizations

Parameters	Hardware utilizations
FPGA	Spartan 6
Slice registers	1,676
Slice LUTs	1,773
Memory	8
occupied slices	667
LUT FF	2,067

In the proposed steganography architecture the X ray image of a patient is embedded with the patient name and date. The simulation results are as shown in Figure 6. The maximum PSNR obtained is 74.28 dB.

The comparision of the proposed method is compared with the existing techniques in Table 3. It is observed that our method obtaines maximum PSNR. To obtain the maximum PSNR we have introduced lossless CDF 5/3 Lift DWT with proper blended to combine the features followed by key generation.

The Table 4 represents the Hardware comparision with the existing techniques. Compared to the methods described by [42], [43], slice registers and LUT FF are better. We achieve optimized hardware utilisations by using effective koggy stone adder/subtractor and vedic multiplier architectures.

Table 3. Comparison of PSNR with existing techniques

Authors	Techniques	Maximum PSNR
AyaJaradat *et al.* [39]	Chaotic particle swarm optimization	69
Muhuri *et al.* [40]	Integer wavelet transformation and particle swarm optimization	52
Mohsin *et al.* [41]	Particle swarm optimization algorithm	58
Proposed	DWT and alpha blending algorithm	74

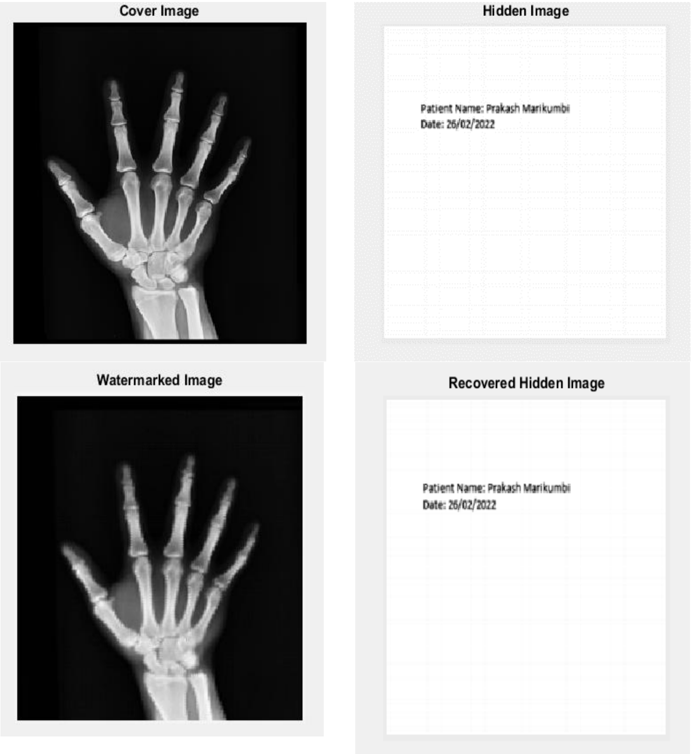

Figure 6. Simulation results

Table 4. Hardware comparison with existing techniques

Parameters	Simha [42]	Jatin and Bhatt [43]	Hardware utilizations
FPGA	Spartan 6	_	Spartan 6
Slice registers	_	2,411	1,676
LUT FF	2,108		2,067

5. CONCLUSION

Medical image protection is crucial to prevent unauthorised and authorised users from changing medical images as well as to maintain confidentiality and address confidentiality concerns. Consequently, it is possible to maintain the security of all forms of data, including medical imaging. Medical picture encryption is a well known method for ensuring the confidentiality of data and images. In this paper, the authors presented a comprehensive and efficient method for encrypting medical photos. Encryption is tested, and hardware utilisations are compared to show effectiveness, for medical images with greater PSNR values.

REFERENCES

[1] A. Anjum *et al.*, "An efficient privacy mechanism for electronic health records," *Computers and Security*, vol. 72, pp. 196–211, Jan. 2018, doi: 10.1016/j.cose.2017.09.014.

[2] M. S. Pour, C. Nader, K. Friday, and E. Bou-Harb, "A comprehensive survey of recent internet measurement techniques for cyber security," *Computers & Security*, vol. 128, p. 103123, May 2023, doi: 10.1016/j.cose.2023.103123.

[3] Y. Himeur, S. S. Sohail, F. Bensaali, A. Amira, and M. Alazab, "Latest trends of security and privacy in recommender systems: A comprehensive review and future perspectives," *Computers and Security*, vol. 118, p. 102746, Jul. 2022, doi: 10.1016/j.cose.2022.102746.

[4] M. Saqib and A. H. Moon, "A systematic security assessment and review of internet of things in the context of authentication," *Computers and Security*, vol. 125, p. 103053, Feb. 2023, doi: 10.1016/j.cose.2022.103053.

[5] A. E. Omolara *et al.*, "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers and Security*, vol. 112, p. 102494, Jan. 2022, doi: 10.1016/j.cose.2021.102494.

[6] F. Ö. Sönmez, C. Hankin, and P. Malacaria, "Decision support for healthcare cyber security," *Computers and Security*, vol. 122, p. 102865, Nov. 2022, doi: 10.1016/j.cose.2022.102865.

[7] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Computers and Security*, vol. 97, p. 101966, Oct. 2020, doi: 10.1016/j.cose.2020.101966.

[8] F. Cohen, "Information system attacks: A preliminary classification scheme," *Computers and Security*, vol. 16, no. 1, pp. 29–46, Jan. 1997, doi: 10.1016/S0167-4048(97)85785-9.

[9] A. Javeed, C. Yilmaz, and E. Savas, "Detector: An approach for detecting, isolating, and preventing timing attacks," *Computers and Security*, vol. 110, p. 102454, Nov. 2021, doi: 10.1016/j.cose.2021.102454.

[10] L. Thomas, I. Gondal, T. Oseni, and S. S. Firmin, "A framework for data privacy and security accountability in data breach communications," *Computers and Security*, vol. 116, p. 102657, May 2022, doi: 10.1016/j.cose.2022.102657.

[11] H. Wang and R. Zhou, "The application of blockchain to electronic health record systems:A review," in *Proceedings - 2021 International Conference on Information Technology and Biomedical Engineering, ICITBE 2021*, Dec. 2021, vol. 97, pp. 397–401, doi: 10.1109/ICITBE54178.2021.00092.

[12] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, Mar. 2018, doi: 10.1016/j.sigpro.2017.10.004.

[13] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Encryption and watermark-treated medical image against hacking disease-An immune convention in spatial and frequency domains," *Computer Methods and Programs in Biomedicine*, vol. 159, pp. 11–21, Jun. 2018, doi: 10.1016/j.cmpb.2018.02.021.

[14] M. T. I. Siyam, K. M. R. Alam, and T. Jami, "An exploitation of visual cryptography to ensure enhanced security in several applications," *Int. Journal of Computer Applications*, vol. 65, no. 6, pp. 42–46, 2013.

[15] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," *Computers and Security*, vol. 92, p. 101752, May 2020, doi: 10.1016/j.cose.2020.101752.

[16] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, "Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption," *IEEE Access*, vol. 9, pp. 25911–25925, 2021, doi: 10.1109/ACCESS.2021.3056037.

[17] M. K. Hasan *et al.*, "Lightweight encryption technique to enhance medical image security on internet of medical things applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021, doi: 10.1109/ACCESS.2021.3061710.

[18] Y. Ding, F. Tan, Z. Qin, M. Cao, K. K. R. Choo, and Z. Qin, "DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 9, pp. 4915–4929, Sep. 2022, doi: 10.1109/TNNLS.2021.3062754.

[19] B. Han, Y. Jia, G. Huang, and L. Cai, "A medical image encryption algorithm based on hermite chaotic neural network," in *Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2020*, 2020, pp. 2644–2648, doi: 10.1109/ITNEC48623.2020.9085079.

[20] S. Haddad, G. Coatrieux, A. Moreau-Gaudry, and M. Cozic, "Joint watermarking-encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2556–2569, 2020, doi: 10.1109/TIFS.2020.2972159.

[21] J. Khan *et al.*, "Medical image encryption into smart healthcare IoT system," in *2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2019*, Dec. 2019, pp. 378–382, doi: 10.1109/ICCWAMTIP47768.2019.9067592.

[22] Y. Ding *et al.*, "DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1504–1518, Feb. 2021, doi: 10.1109/JIOT.2020.3012452.

[23] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography," *Information Security Journal*, vol. 29, no. 2, pp. 91–101, Mar. 2020, doi: 10.1080/19393555.2020.1718248.

[24] R. Maurya, A. K. Kannojiya, and B. Rajitha, "An extended visual cryptography technique for medical image security," in *2nd International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2020 - Conference Proceedings*, Mar. 2020, pp. 415–421, doi: 10.1109/ICIMIA48430.2020.9074910.

[25] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Medical and Biological Engineering and Computing*, vol. 57, no. 11, pp. 2517–2533, Nov. 2019, doi: 10.1007/s11517-019-02037-3.

[26] S. Priya and B. Santhi, "A novel visual medical image encryption for secure transmission of authenticated watermarked medical images," *Mobile Networks and Applications*, vol. 26, no. 6, pp. 2501–2508, Dec. 2021, doi: 10.1007/s11036-019-01213-x.

[27] Z. Mishra and B. Acharya, “High throughput and low area architectures of secure IoT algorithm for medical image encryption,” *Journal of Information Security and Applications*, vol. 53, p. 102533, Aug. 2020, doi: 10.1016/j.jisa.2020.102533.

[28] A. S. Banu and R. Amirtharajan, “A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach,” *Medical and Biological Engineering and Computing*, vol. 58, no. 7, pp. 1445–1458, Jul. 2020, doi: 10.1007/s11517-020-02178-w.

[29] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, “Medical image encryption algorithm based on Latin square and memristive chaotic system,” *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 35419–35453, Dec. 2019, doi: 10.1007/s11042-019-08168-x.

[30] J. C. Dagadu, J. P. Li, and E. O. Aboagye, “Medical image encryption based on hybrid chaotic DNA diffusion,” *Wireless Personal Communications*, vol. 108, no. 1, pp. 591–612, Sep. 2019, doi: 10.1007/s11277-019-06420-z.

[31] K. Andra, C. Chakrabarti, and T. Acharya, “A VLSI architecture for lifting-based forward and inverse wavelet transform,” *IEEE Transactions on Signal Processing*, vol. 50, no. 4, pp. 966–977, Apr. 2002, doi: 10.1109/78.992147.

[32] O. Evsutin, A. Melman, and R. Meshcheryakov, “Digital steganography and watermarking for digital images: A review of current research directions,” *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.

[33] S. Sarkar and S. S. Bhairannawar, “Efficient FPGA architecture of optimized haar wavelet transform for image and video processing applications,” *Multidimensional Systems and Signal Processing*, vol. 32, no. 2, pp. 821–844, Apr. 2021, doi: 10.1007/s11045-020-00759-4.

[34] V. Anbumani, S. Soviya, S. Sneha, and L. Saran, “Speed and power efficient vedic multiplier using adders with MUX,” in *3rd IEEE International Virtual Conference on Innovations in Power and Advanced Computing Technologies, i-PACT 2021*, Nov. 2021, pp. 1–5, doi: 10.1109/i-PACT52855.2021.9696992.

[35] F. Liu and W. Q. Yan, *Visual cryptography for image processing and security: Theory, methods, and applications*, vol. 9783319096. 2014.

[36] Digilent, “Datasheet of Digilent ATLYS FPGA board.” 2016, [Online]. Available: https://reference.digilentinc.com/_media/atlys:atlys:atlys_rm.pdf.

[37] S. T. Karris, *Introduction to siuink with engineering applications*, 2nd ed. Gatesmark Publishing, 2006.

[38] C. H. Roth, *Teaching digital system design using VHDL*. Cengage Learning, 1994.

[39] A. Jaradat, E. Taqieddin, and M. Mowafi, “A high-capacity image steganography method using chaotic particle swarm optimization,” *Security and Communication Networks*, vol. 2021, pp. 1–11, Jun. 2021, doi: 10.1155/2021/6679284.

[40] 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 Journal*, vol. 92, p. 106257, Jul. 2020, doi: 10.1016/j.asoc.2020.106257.

[41] A. H. Mohsin *et al.*, “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, doi: 10.1109/ACCESS.2019.2949622.

[42] H. N. N. Simha, P. M. Prakash, S. S. Kashyap, and S. Sarkar, “FPGA implementation of image steganography using Haar DWT and modified LSB techniques,” in *2016 IEEE International Conference on Advances in Computer Applications, ICACA 2016*, Oct. 2017, pp. 26–31, doi: 10.1109/ICACA.2016.7887918.

[43] J. Chaudhari and K. R. Bhatt, “FPGA Implementation of Image Steganography: A retrospective,” *International Journal of Engineering Development and Research*, vol. 2, no. 2, pp. 2117–2121, 2014.

BIOGRAPHIES OF AUTHORS

Prakash Marakumbi is working as a faculty in the department of electronics and communication engineering at Tontadarya College of Engineering, Gadag, Karnataka, India. He has completed B.E. from SDM College of Engineering and Technology, Dharwad, India and M.Tech. from UBDT College of Engineering, Davangere, India. He can be contacted at email: pmarakumbi@gmail.com.

Dr. Satish Bhairannawar is the dean of Industry Institute Interface (III), and professor of electronics and communication engineering, SDM College of Engineering and Technology, Dharwad, India. He has been recognized with young researcher award in the year 2017 by InSc (An ISO 9001: 2015 certified institute by international accurate certification, accredited by UASI) and conferred with the title senior member, IEEE for personal and professional commitment to the advancement of technology by IEEE, USA. He can be contacted at email: satishbhairannawar@gmail.com.