


Article

A New Symmetric Image Encryption Scheme based on Block Level Processing using Hash Function and AES

R. Thenmozhi¹, Sivaram Rajeyagari² and S. Balamuralitharan^{3,*} 

¹ Assistant Professor, Department of CSE, SRM Institute of Science and Technology, Kattankulathur, Chennai, India; thenmozr@srmist.edu.in

² Associate Professor, Department of CS, College of Computing and Information Technology, Shaqra University, Saudi Arabia; dr.sivaram@su.edu.sa

³ Assistant Professor, Department of Mathematics, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur-603 203, Chengalpattu District, Tamil Nadu, India; balamurs@srmist.edu.in

Abstract: Data could be in many forms like text, image, audio, video and many others. Amongst these data, processing image is of important concern even with sophisticated technologies. Generally, images consume more storage space and processing time. This work aims in attaining a novel image encryption strategy that consumes very less computational time with maximum security. The idea is to split the image into blocks and rearrange the pixels in diagonal fashion to achieve confusion. Next, the blocks are combined to form sub images and one block of the sub image is subjected to Secure Hash Algorithm (SHA 512 bits). The SHA bits are XORed with the remaining blocks of the sub image. Finally, the entire image is encrypted using Advanced Encryption Standard (AES). Decryption process is the exact reverse of encryption process. The computational overhead is very low, and security is efficient. The results are compared with existing encryption techniques.

Keywords: Encryption; Decryption; Security; SHA; AES

1. Introduction

Nowadays, data owners who could not afford to have a storage space for their data, lookup to common storage spaces to maintain their data. In this case, data must be outsourced, and this demands security for the data that is to be stored in a remote location. Image security is still of concern when it comes to outsourcing. Images include sensitive information as in case of medical images. There are many existing image encryption strategies achieving different levels of security.

In [1], Zhongyun Hua et al., have presented an image encryption technique using filtering technology and Josephus problem. The Josephus problem is employed to add confusion and filtering technique is for diffusion in the encryption method. Qing Lu et al., in [2], have introduced chaotic S-box based encryption technique for images. The authors have also cryptanalyzed using chosen plaintext attack and have improved the S box security using the cryptanalytic knowledge. In [3], Xingyuan et al. have studies chaotic encryption techniques used for images. The authors have utilized a Boolean network encryption algorithm and tensor product theory using matrix for image encryption.

Khan Muhammad et al. in [4], has used image encryption in IoT application for surveillance using video summarization. The video captured from the sensors are converted into frames and are considered as images which is then encrypted. Xiuli Chai et al., in [5] have used Elementary Cellular Antenna (ECA), Compressive System and Chaotic System for image encryption. Discrete Wavelet Transform (DWT) and SHA are also employed for security purpose. Shuqin Zhu et al. [6] have proposed an image

encryption scheme that utilizes block level processing mechanism and chaotic system. To achieve confusion, scrambling is performed, and two levels of diffusion mechanisms are incorporated.

Medical image security system using chaotic functions were introduced by Shankar et al. in [7]. The authors have used tent maps and chaotic logistics to analyse the keys of secure medical images. Sara Farrag et al. in [8] have presented a three-level security system for images. The idea is a zigzag embedding pattern. AES algorithm is used for encryption in the first layer, chaotic function-based encryption in the second layer. In third layer, Least Significant Bit (LSB) based zigzag embedding is carried out to achieve image steganography. Optimization based cryptographic technique for image encryption in IoT is presented by Mohamed Elhoseny et al. [9]. The objective of this work is to achieve secure encryption and transmission of medical images. Key selection is done using grasshopper optimization technique in Elliptic Curve Cryptography (ECC).

Mohammed Es-Sabbry et al. in [10] have introduced an encryption technique for images that uses random number generators and bitwise shift operators. This method is well suited for colour images. Watermarking strategies are combined with encryption mechanisms to provide security for medical images in [11]. This is a hybrid approach. The authors have also specified methods to verify authenticity and integrity of the encrypted images. Ziad E. Dawahdeh et al. in [12] have presented Elliptic Curve Cryptography (ECC) and Hill cipher-based encryption scheme for images. This is a symmetric key based encryption mechanism to secure images in an efficient way. In [13], Ibrahim Yasser et al. have used chaotic functions for encryption. The authors have given a perturbation algorithm and have also used chaotic systems twice. The chaotic functions include Discrete Wavelet Transform (DWT) and permutation.

2. Proposed Method

2.1. Encryption Phase

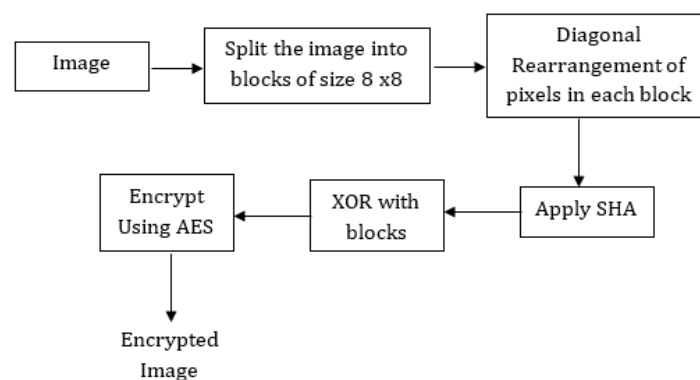


Figure 1. Image Encryption Phase

The process of encrypting the image is shown in Figure 1. Split the image that is to be encrypted into blocks of size 8×8 . Rearrange the pixels of each 8×8 image block in diagonal order. This pixel diagonal rearrangement process is depicted in Figure 2.

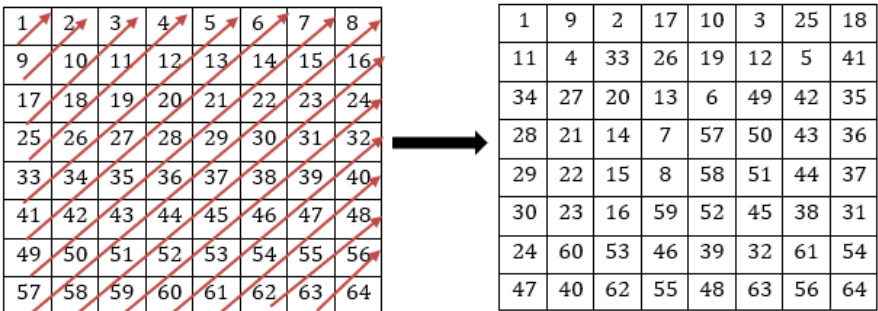


Figure 2. Diagonal Rearrangement of pixels

Repeat this diagonal rearrangement process for all the 8x8 image blocks. Now we obtain a rearranged image. Next split the image again into blocks of size 8x8. For processing, consider 4 blocks as one sub image. Example, if the input image is of size 64x64, when it is split into blocks of size 8x8, 64 such blocks are formed. Here four blocks are taken as one sub image, thereby forming 16 sub images. This is illustrated in Figure 3. Among the four blocks, the last block is subjected to Secure Hash Algorithm (512 bits) and is XORed with the remaining three blocks. Each 8x8 block contains 64 pixels and when each of these pixels are converted into binary, they create 512 bits (64 x 8). These 512 bits are XORed with the SHA bits. This process is repeated for all the sub images.

B1	B2	B3	B4	B5	B6	B7	B8
B9	B10	B11	B12	B13	B14	B15	B16
B17	B18	B19	B20	B21	B22	B23	B24
B25	B26	B27	B28	B29	B30	B31	B32
B33	B34	B35	B36	B37	B38	B39	B40
B41	B42	B43	B44	B45	B46	B47	B48
B49	B50	B51	B52	B53	B54	B55	B56
B57	B58	B59	B60	B61	B62	B63	B64

(a) Image split into blocks of size 8x8

SUB IMAGE 1		SUB IMAGE 2		SUB IMAGE 3		SUB IMAGE 4	
B1	B2	B3	B4	B5	B6	B7	B8
B9	B10	B11	B12	B13	B14	B15	B16
SUB IMAGE 5		SUB IMAGE 6		SUB IMAGE 7		SUB IMAGE 8	
B17	B18	B19	B20	B21	B22	B23	B24
B25	B26	B27	B28	B29	B30	B31	B32
SUB IMAGE 9		SUB IMAGE 10		SUB IMAGE 11		SUB IMAGE 12	
B33	B34	B35	B36	B37	B38	B39	B40
B41	B42	B43	B44	B45	B46	B47	B48
SUB IMAGE 13		SUB IMAGE 14		SUB IMAGE 15		SUB IMAGE 16	
B49	B50	B51	B52	B53	B54	B55	B56
B57	B58	B59	B60	B61	B62	B63	B64

(b) Image blocks represented as Sub images

Figure 3. Image split as blocks and Sub images

In each of the sub images, the last block is subjected to SHA 512 bits and is XORed with the remaining blocks of the same sub image, whereas, the blocks that are subjected to SHA are left unaltered. Example, in sub image 1, the blocks are B1, B2, B9 and B10. Here, SHA is applied on B10 and the result is XORed with B1, B2, B9 and the block B10 is left unaltered.

After repeating this process for all the sub images, the entire image is encrypted using Advanced Encryption Standard (AES). Out of the available standard encryption algorithms, AES is very strong and best suited for image encryption.

2.2. Decryption Phase

The decryption process is exactly the reverse of encryption process and is shown in Figure 4. The output image of the encryption process is first decrypted using AES. This decrypted image is then split into blocks and formed as sub images. Blocks are of size 8x8 and four blocks form a sub image. The last block of the sub image is applied with SHA and the result is XORed with remaining three blocks of the same sub image.

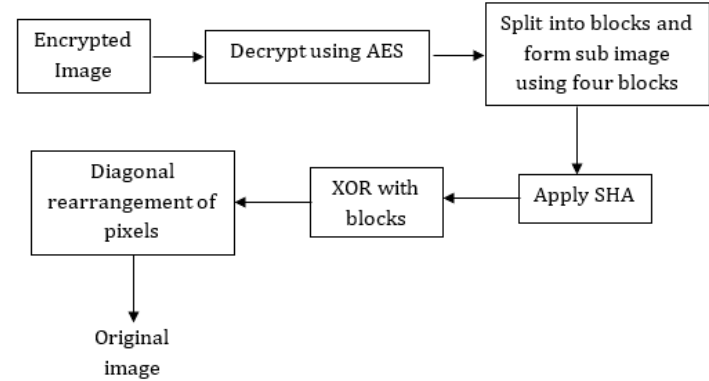


Figure 4. Image Decryption Phase

This idea is based on the following property of XOR,

$$A \oplus B \oplus B = A$$

here, let A be the original block and B is the SHA output of the last block of the sub image. In encryption phase, they are XORed as $A \oplus B$. In decryption phase, this value is again XORed with B which will give the original A value.

Finally, each of the 8x8 block is diagonally rearranged to obtain the original image as shown in Figure 5. The values are read row wise and arranged diagonally.

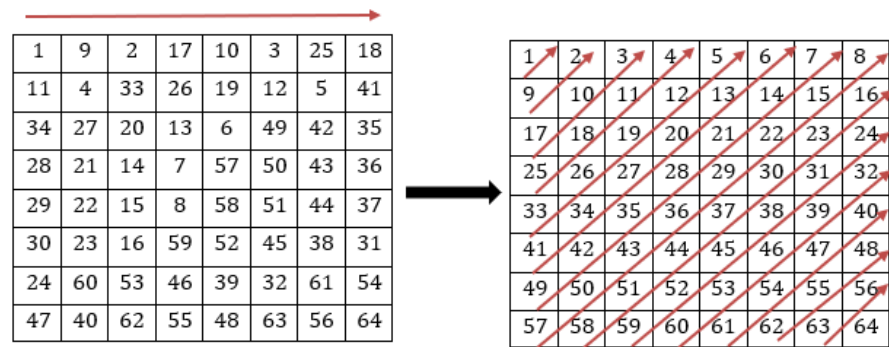


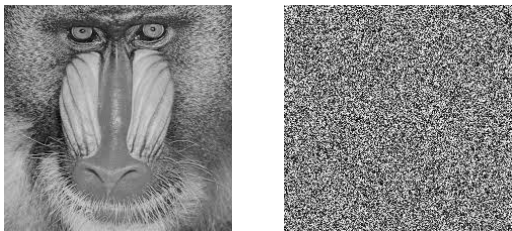
Figure 5. Diagonal rearrangement of pixels in decryption phase

3. Experimants and Results

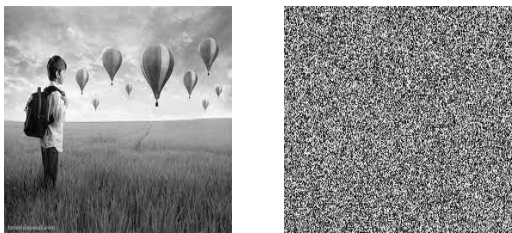
The proposed encryption scheme has been tested with various standard images used for testing in image processing. Here, in this work, we have shown the results of eight images from the standard images like the Apple, Baboon, Balloon, Camera man, Einstein, House, Lena, Peppers and two medical images Kidney and chest. These images in sizes of 64x64, 128x128, 256x256 and 512x512 are taken for experimentation. The encryption and decryption time (in milliseconds) for the above mentioned ten images are tabulated in Table 1. The original images and their encrypted forms are shown in Figure 6.



(a) Apple image and its Encrypted Image



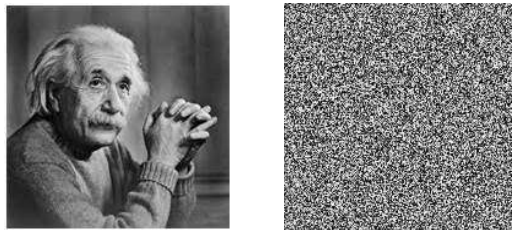
(b) Baboon image and its Encrypted Image



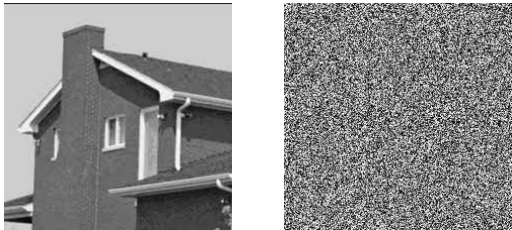
(c) Balloon image and its Encrypted Image



(d) Camera man image and its Encrypted Image



(e) Einstein image and its Encrypted Image



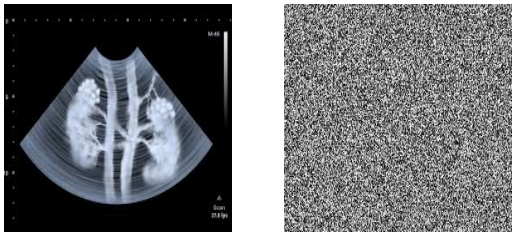
(f) House image and its Encrypted Image



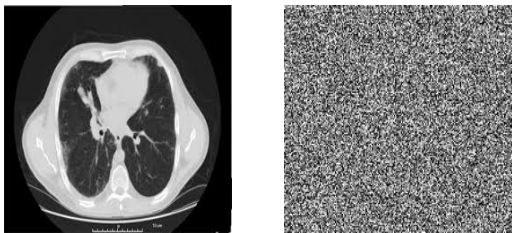
(g) Lena image and its Encrypted Image



(h) Peppers image and its Encrypted Image



(i) Kidney image and its Encrypted Image



(j) Chest image and its Encrypted Image

Figure 6 Original images and its corresponding encrypted images

Table 1. Encryption and Decryption times of the proposed scheme

Image	Image Size	No. of Blocks	No. of Sub Images	Encryption Time (in ms)	Decryption Time (in ms)
Apple	64x64	64	16	31	33
	128x128	256	64	35	36
	256x256	1024	256	41	44
	512x512	4096	1024	47	50
Baboon	64x64	64	16	32	35
	128x128	256	64	36	39
	256x256	1024	256	40	45
	512x512	4096	1024	49	51
Balloon	64x64	64	16	32	34
	128x128	256	64	35	38
	256x256	1024	256	42	46
	512x512	4096	1024	48	52
Camera man	64x64	64	16	31	36
	128x128	256	64	36	39
	256x256	1024	256	39	43
	512x512	4096	1024	45	49
Einstein	64x64	64	16	33	35
	128x128	256	64	37	40
	256x256	1024	256	41	44
	512x512	4096	1024	46	52
House	64x64	64	16	32	34
	128x128	256	64	36	38
	256x256	1024	256	40	44
	512x512	4096	1024	45	47
Lena	64x64	64	16	34	37
	128x128	256	64	38	42
	256x256	1024	256	42	45
	512x512	4096	1024	46	51
Peppers	64x64	64	16	33	36
	128x128	256	64	37	41
	256x256	1024	256	42	46
	512x512	4096	1024	48	53
Kidney	64x64	64	16	32	36
	128x128	256	64	35	40
	256x256	1024	256	40	44
	512x512	4096	1024	46	53
Chest	64x64	64	16	31	33
	128x128	256	64	35	37
	256x256	1024	256	39	44
	512x512	4096	1024	44	49

The comparative analysis of the encryption and decryption times of the proposed scheme is shown as graphs in Figure 7. The comparison is made for all sizes of image taken into consideration i.e., 64x64, 128x128, 256x256, 512x512.

In [5], a chaotic system and compressive sensing-based encryption technique is suggested and in [7], a key based chaotic function is used for medical image encryption. The proposed scheme in this work is compared with these existing systems and it could be observed that the proposed work is far better than the existing similar works in terms of computational complexity and security. The comparison of encryption times is tabulated in Table 2 and comparison of decryption times is tabulated in Table 3.

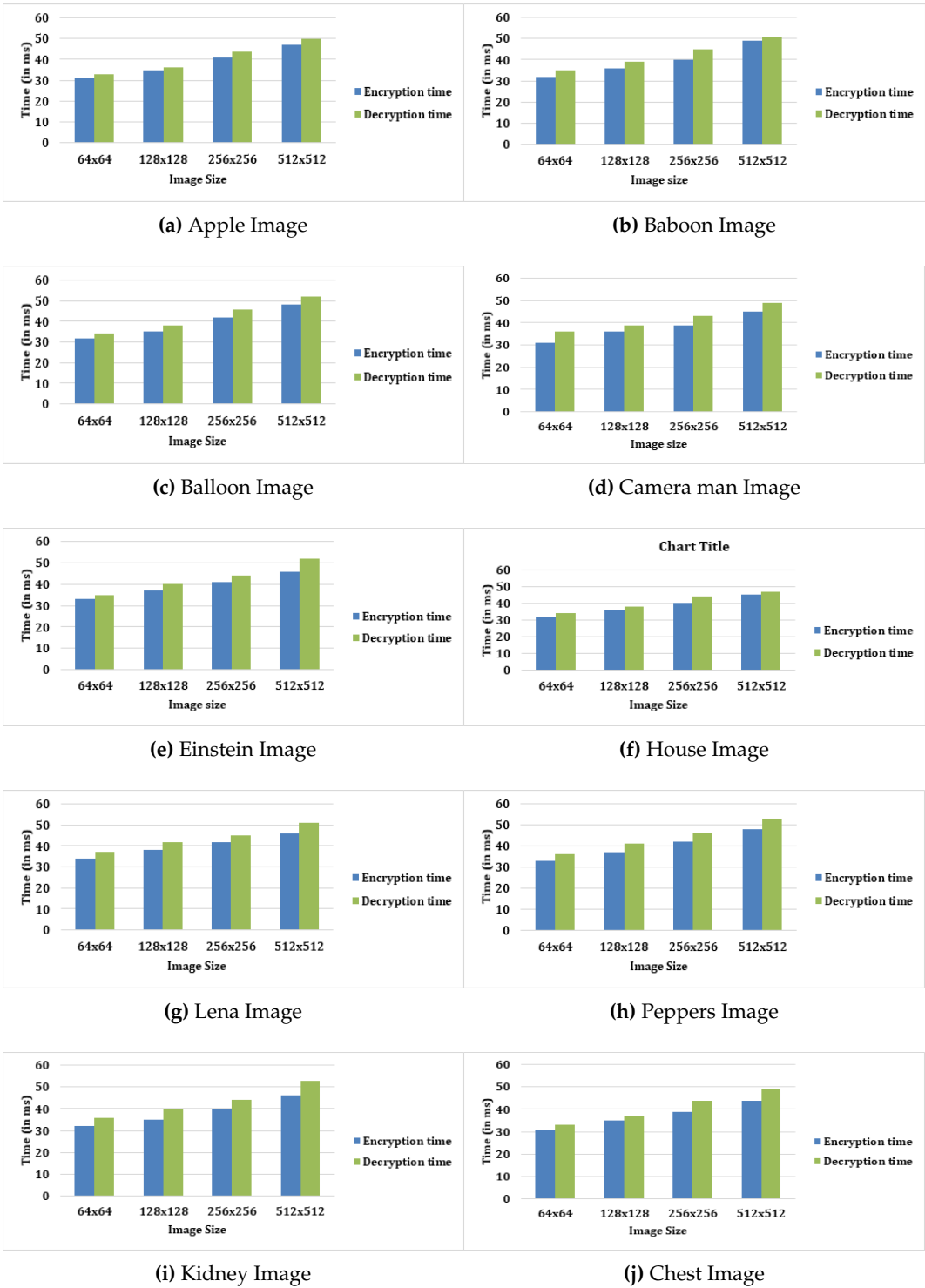


Figure 6. Comparative analysis of encryption and decryption times

Table 2. Encryption Time comparison

Image	Image Size	Encryption Time (in ms)		
		Proposed Method	Reference[5]	Reference[7]
Apple	64x64	31	33	34
	128x128	35	38	40
	256x256	41	45	47
	512x512	47	50	58
Baboon	64x64	32	36	39
	128x128	36	41	47
	256x256	40	44	46
	512x512	49	53	57
Balloon	64x64	32	35	39
	128x128	35	38	42
	256x256	42	46	51
	512x512	48	53	55
Camera man	64x64	31	35	37
	128x128	36	39	44
	256x256	39	45	49
	512x512	45	49	54
Einstein	64x64	33	38	44
	128x128	37	42	46
	256x256	41	47	51
	512x512	46	51	57
House	64x64	32	36	41
	128x128	36	42	47
	256x256	40	45	49
	512x512	45	48	54
Lena	64x64	34	36	38
	128x128	38	40	44
	256x256	42	45	48
	512x512	46	49	54
Peppers	64x64	33	37	42
	128x128	37	41	46
	256x256	42	47	51
	512x512	48	52	55
Kidney	64x64	32	37	42
	128x128	35	39	44
	256x256	40	46	55
	512x512	46	52	57
Chest	64x64	31	35	37
	128x128	35	39	44
	256x256	39	44	48
	512x512	44	49	53

Table 3. Decryption Time comparison

Image	Image Size	Decryption Time (in ms)		
		Proposed Method	Reference[5]	Reference[7]
Apple	64x64	33	35	38
	128x128	36	39	42
	256x256	44	46	49
	512x512	50	54	59
Baboon	64x64	35	39	42
	128x128	39	43	47
	256x256	45	49	55
	512x512	51	56	61
Balloon	64x64	34	37	40
	128x128	38	42	45
	256x256	46	49	53
	512x512	52	56	59
Camera man	64x64	36	39	43
	128x128	39	43	47
	256x256	43	48	52
	512x512	49	53	57
Einstein	64x64	35	39	44
	128x128	40	45	50
	256x256	44	47	51
	512x512	52	55	58
House	64x64	34	38	42
	128x128	38	41	44
	256x256	44	48	52
	512x512	47	51	56
Lena	64x64	37	40	45
	128x128	42	43	47
	256x256	45	47	49
	512x512	51	52	56
Peppers	64x64	36	41	44
	128x128	41	43	47
	256x256	46	49	53
	512x512	53	57	60
Kidney	64x64	36	39	42
	128x128	40	42	45
	256x256	44	47	50
	512x512	53	56	59
Chest	64x64	33	37	40
	128x128	37	39	42
	256x256	44	46	49
	512x512	49	54	58

3.1. Security Analysis

The security of the proposed encryption scheme lies in the security efficiency of the AES algorithm. It is well known that the AES algorithm is a standard encryption scheme that still has no efficient cryptanalytic techniques to completely break it in polynomial time. AES 128 bits can be recovered with time complexity $2^{126.1}$ using biclique attack. Also, this attack can recover keys of AES 192 bits and AES 256 bits with time complexity $2^{189.7}$ and $2^{254.4}$. Another attack called related key attack makes AES 192 bits and AES 256 bits vulnerable with time complexity $2^{99.5}$ and 2^{176} correspondingly. Though these are provable possible attacks, the computational overhead for these attacks is not practical.

In the proposed scheme, diagonal rearrangement of pixels is done to achieve confusion and XORing with SHA 512 bits will infuse diffusion to the encryption scheme. To measure the efficiency of the proposed encryption methodology, we have used a metric called Unified Average Changing Intensity (UACI). The encryption scheme is said to be resistive against differential attacks if the UACI value is high. The mathematical expression of UACI is as follows,

$$UACI = \frac{1}{128 \times 128} \sum_{i=1}^{128} \sum_{j=1}^{128} \frac{|x(i,j) - y(i,j)|}{127} \times 100\%$$

where $x(i,j)$ represents the pixels of original image and $y(i,j)$ represents pixels of the duplicate image. This formula is for a 128 X 128 sized image. If the image is of different dimensions, then the summation limits and denominator changes according to it. The UACI values for the proposed method is recorded and presented in Table 4. The recorded values are for the test images of size 128 x 128 and the observation is that the encryption scheme is very efficient since the values are high and good.

Table 4. UACI values for the images encrypted with proposed method

Image	UACI Value
Apple	31.33
Baboon	30.46
Balloon	31.68
Camera man	32.45
Einstein	31.87
House	30.56
Lena	30.89
Peppers	31.56
Kidney	31.86
Chest	30.93

4. Conclusions

An efficient encryption scheme for image security is presented in this paper. The encryption methodology mentioned in this work is more efficient than the existing works and the UACI value that determines the strength of the encryption scheme is also high. The proposed method ensures the two most important attributes for any encryption method – Confusion and Diffusion. Confusion is achieved through pixel rearrangement and diffusion is achieved through XORing the SHA bits. Further AES, which is one of the strongest encryption method is used in this work. This methodology works well for images of all sizes and they are also well suited for medical images.

References

1. Z. Hua, B. Xu, F. Jin, H. Huang, Image encryption using josephus problem and filtering diffusion, *IEEE Access* 7 (2019) 8660–8674.
2. Q. Lu, C. Zhu, X. Deng, An efficient image encryption scheme based on the lss chaotic map and single s-box, *IEEE Access* 8 (2020) 25664–25678.
3. X. Wang, S. Gao, Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory, *Information sciences* 507 (2020) 16–36.
4. K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, S. W. Baik, Secure surveillance framework for iot systems using probabilistic image encryption, *IEEE Transactions on Industrial Informatics* 14 (8) (2018) 3679–3689.
5. X. Chai, X. Zheng, Z. Gan, D. Han, Y. Chen, An image encryption algorithm based on chaotic system and compressive sensing, *Signal Processing* 148 (2018) 124–144.
6. S. Zhu, C. Zhu, Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map, *IEEE Access* 7 (2019) 147106–147118.

7. K. Shankar, M. Elhoseny, E. D. Chelvi, S. Lakshmanaprabu, W. Wu, An efficient optimal key based chaos function for medical image security, *IEEE Access* 6 (2018) 77145–77154.
8. S. Farrag, W. Alexan, H. H. Hussein, Triple-layer image security using a zigzag embedding pattern, in: 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), IEEE, 2019, pp. 1–8.
9. M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maselena, N. Arunkumar, Hybrid optimization with cryptography encryption for medical image security in internet of things, *Neural computing and applications* (2018) 1–15.
10. M. Es-Sabry, N. El Akkad, M. Merras, A. Saaïdi, K. Satori, A new image encryption algorithm using random numbers generation of two matrices and bit-shift operators, *Soft Computing* 24 (5) (2020) 3829–3848.
11. A. Al-Haj, H. Abdel-Nabi, Digital image security based on data hiding and cryptography, in: 2017 3rd International conference on information management (ICIM), IEEE, 2017, pp. 437–440.
12. Z. E. Dawahdeh, S. N. Yaakob, R. R. bin Othman, A new image encryption technique combining elliptic curve cryptosystem with hill cipher, *Journal of King Saud University-Computer and Information Sciences* 30 (3) (2018) 349–355.
13. I. Yasser, F. Khalifa, M. A. Mohamed, A. S. Samrah, A new image encryption scheme based on hybrid chaotic maps, *Complexity* 2020 (2020).