Research Article

HYBRID BAKER MAP WITH AES IN CIPHER BLOCK CHAINING MODE IN MEDICAL IMAGES

Amudha K ^{*1}, Nelson Kennedy Babu C ², Balu S ³

¹Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India

²Department of Computer Science and Engineering, Dhanalakshmi Srinivasan College of Engineering, Coimbatore, Tamil Nadu, India

³Department of Computer Science and Engineering, K. S. Rangasamy College of Technology, Namakkal, Tamil Nadu, India

*Corresponding Author Email: amudhak02 @gmail.com

Article Received on: 13/03/17 Approved for publication: 20/04/17

DOI: 10.7897/2230-8407.080451

ABSTRACT

While transferring the medical images from one place to another place lot of security issues are raised. The security issues are confidentiality, integrity and authenticity. Combined encryption and watermarking technique used to verify the integrity and authenticity of medical images. Encryption algorithms are operated in stream cipher and block cipher mode. Advanced Encryption Standard (AES) algorithm is one of the block cipher algorithm. The proposed method uses Advanced Encryption Standard Algorithm in Cipher Block Chaining (CBC) mode. To increase the security, the proposed technique uses baker key in the original image before applying the AES algorithm. Based on the baker key the image pixel position has been changed. To increase the data hiding capacity this technique embeds the information in the spatial domain and encrypted domain. The main objective of this method is to provide integrity and authenticity of the medical images at the same time increase the information embedding capacity. Experimental security analysis is taken for the 8-bit ultrasound images and 16-bit Positron Emission Tomography (PET) images.

Keywords: Integrity, Authenticity, Spatial domain, Encrypted domain, AES in CBC

INTRODUCTION

Medical imaging plays a vital role in telesurgery, telemedicine, telediagnosis and so on. Media and telecom advances require a diverse method for remote access and sharing of patient information. Even though the transmission is easy, it lacks in few security metrics such as confidentiality, availability and reliability¹. Cryptographic algorithms are used to provide data confidentiality and integrity in information systems. The medical information is left, if the decrypted or digital signature is lost and it is not easy to verify its integrity and origin. So, the cryptographic algorithms are considered as a priori protection technique.

In order to improve the security of medical images the watermarking techniques are used with an encryption method². The joint encryption and watermarking technique is used to protect the information. The reliability of the same is verified by asserting its integrity and authenticity. During the transaction, the Patient Health Record (PHR) that contains patient name and physician identity can be inserted into an image by using a watermarking method otherwise posterior technique³. The combined priori and posteriori technique is used to enhance the security in medical images^{4,5}.

Normally, RC6 block cipher algorithm is used to encrypt the data^{6,7}. AES block cipher supports large size of data compared to RC6 block cipher. Hence, AES is used in the proposed methodologies in Cipher Block Chaining (CBC) mode. AES is a block cipher method that operates on discrete blocks

of data using a fixed key. A high embedding capacity rate is achieved because of double watermarking and double AES is used for encryption to increase security which leads to a complex workaround⁸. To reduce complexity of work and time, a better methodology is proposed in this paper. Here, secret information is embedded in the spatial domain and encrypted domain simultaneously with AES algorithm used in CBC mode for encryption purpose leading to better security.

MATERIALS AND METHODS

Hybrid Baker Map with AES in CBC Mode

Information with authenticity code is embedded in both spatial domain and encrypted domain in the original input image⁹. This authenticity code is used to identify the image origin and an integrity proof. Then the resultant watermarked image has been encrypted by AES with the help of the secret key.

In the proposed system, Baker Map algorithm is used before embedding the information into spatial domain and encrypted domain. The Baker Map algorithm divides the square matrix of the original image into rectangles with different sizes. Then the baker map algorithm modifies the pixel position of the original image based on the baker key.

After that, the information has been inserted in two ways into spatial domain and encrypted domain. The information is encoded parallel in the spatial domain and encrypted domain with different authenticity code. The output image, after embedding is called as watermarked image, which is further

encrypted by AES in cipher block chaining mode to get encrypted image. The overall flow diagram of the proposed method is shown in Figure 1.

Figure 1: Flow diagram of hybrid baker map with AES in CBC mode

Baker Map Algorithm

The baker map is utilized as a preprocessing apparatus to build the security of the system. It is a permutation based technique, which is carried out the randomization of a square matrix of dimensions (M X M) by changing the pixel positions in view of the secret key. It assigns a pixel to another pixel position in a bijective way. The square matrix is partitioned into rectangles with various sizes of the width and number of components. The

components in every rectangle are revised to a row in the permuted rectangle. Rectangles are taken from right to left start with upper rectangles and after that lower ones. Inside every rectangle, the scan starts from the base left corner towards upper components^{10,11}. A Baker map algorithm with key [2 4 2] is shown in Figure 2.

Pixel position is changed by the baker map algorithm with respect to keys.

Here, Pixels in rectangles are taken from right upper rectangles followed by bottom ones. Inside every rectangle, the output starts from the base left corner towards upper components that are located in the first row of the reordered table. In this above example, right upper rectangles bottom pixel of left corner is P31 which is the first element of the first row. Next bottom left corner towards upper element is P23 which comes as second element of the first row in the reordered table, likewise the all elements in the first row are filled. For second row, the next rectangle on the right side is its bottom one, the bottom element is P63 it comes to the first element of the second row likewise the second row is filled. For the third row, the right side upper rectangle left corner bottom element is P11, which comes as first element of the third row, likewise the third row is filled. Similarly, pixels are filled in all rows^{12,13}.

P1	P2	P3	P4	P5	P6	P7	P8
P9	P10	P11	P12	P13	P14	P15	P16
P17	P18	P19	P20	P21	P22	P23	P24
P25	P26	P27	P28	P29	P30	P31	P32
P33	P34	P35	P36	P37	P38	P39	P40
P41	P42	P43	P44	P45	P46	P47	P48
P49	P50	P51	P52	P53	P54	P55	P56
P57	P58	P59	P60	P61	P62	P63	P64

↓

P31	P23	P15	P7	P32	P24	P16	P8
P63	P55	P47	P39	P64	P56	P48	P40
P11	P3	P12	P4	P13	P5	P14	P6
P27	P19	P28	P20	P29	P21	P30	P22
P43	P35	P44	P36	P45	P37	P46	P38
P59	P51	P60	P52	P61	P53	P62	P54
P25	P17	P9	P1	P26	P18	P10	P2
P57	P49	P41	P33	P58	P50	P42	P34

Figure 2: Baker key [2 4 2]

ENCRYPTION

Block Cipher Algorithm

Block cipher algorithms are generally used to encode large size of information in terms of blocks. Block ciphers are working in various modes to achieve better security. The modes of operation of block ciphers are configuration methods that permit those ciphers to work with extensive information streams, without the risk of compromising the security. However, it is possible while working with block ciphers, to use the same secret key bits for encrypting the same plain text. A deterministic algorithm is utilized for multiple data input streams, resulting in a number of the same cipher text blocks. It is an extremely hazardous circumstance for the cipher's clients. An intruder would be able to get much information knowing a distribution of indistinguishable message parts, even if would not be able to break the cipher and discover the original messages. There exist some approaches to blur the cipher output. The idea is to mix the plain text blocks with the cipher text blocks and use the outcome as the cipher input. As a result,

the user avoids creating indistinguishable output cipher text blocks from the same input data. These modifications are called the block cipher modes of operations^{14,15}.

The modes of operation are characterized as Electronic Code Book, Cipher Feedback, Cipher Block Chaining, Counter and Output Feedback. In the proposed technique use the Cipher Block chaining mode in the AES algorithm to encrypt the data¹⁶.

AES Encryption in CBC mode

A plaintext block is combined with the previous cipher text block through XOR operation when CBC mode is applied. B_i^e is denoted as an encrypted version of block B_i and B_{i-1}^e refers the previous encrypted block, hence it is given by

$$B_i^e = \text{AES}(B_i \text{ XOR } B_{i-1}^e, K_e)$$

Where, K_e is the Encryption Key. AES in cipher block chaining mode operation is shown in Figure 3.

Figure 3: AES in CBC mode

The previous cipher text block is exclusive ORed with the current plain text block (B_1) to get an encrypted version of that plain text (B_1^e), and then this output is encrypted by AES with a secret key to get cipher text and so on.

Combined Encryption And Watermark

The main objective of this system is to verify the reliability of an image within the spatial domain and encrypted domain. The combined watermarking and encryption approach is shown in Figure 4.

Figure 4: Combined approach

In this watermarking technique, information is embedded in the spatial domain and encrypted domain. In the spatial domain, information is embedded with Authenticity Code (AC) and Secure Hash code. This authenticity code is used to verify the patient authentication and secure hash code is used to verify the integrity proof^{17,18}. The spatial domain messages (Msg_s) contain authenticity code and secure hash code.
 $(Msg_s) = \langle AC, SHA \text{ code} \rangle$

In encrypted domain, information is embedded with authenticity code and Pseudo random sequence of bits generated by encrypting watermarking key (K_w^e). Here, Pseudo random sequences of bits verify the integrity as well as authenticity code verifies the authenticity. Encrypted domain message (Msg_e) represented as

$Msg_e = \langle AC, PRNG \text{ bits} \rangle$

Here, information has been embedded in the spatial domain as well as the encrypted domain is used to increase the embedding capacity rate. At the same time, secure hash code and PRNG bits with authenticity code is included in the message to provide more authenticity and integrity. Here, secret information is embedded in spatial end encrypted domain which is represented as double watermark.

RESULTS

Experimental results are conducted on Ultrasound images and Positron Emission Tomography (PET) images. The sample image sets are shown in the Figure 5.

Figure 5: Sample images

Baker map algorithm is applied to the original Ultrasound and PET images which changes the pixel position. The original ultrasound image and PET images are taken for experimental purpose is shown in Figure 6 (a) and baker key [2 4 2] is applied

on the images then the pixel position is changed which is shown in Figure 6(b). Next baker key [4 8 4] is applied to the images, the changed pixel position is shown in Figure 6 (c).

Figure 6: Resultant images using different baker key

The resultant encrypted image using AES in CBC mode is shown in Figure 7. Advanced AES in CBC mode refers that a plaintext block is combined with the previous cipher text block through an XOR operation before being encrypted. The original PET image, watermarked encrypted image and decrypted image are shown in Figure 7 (a), (b) and (c) respectively.

Figure 7: Evaluated images using AES

Figure 8: Histogram analysis of PET image

In order to verify its integrity, histogram analysis is taken for original input images and decrypted images. Histogram analysis is taken for original input PET image 6(a) and baker image 6(b) and its encrypted image 7(b), in encryption side and decryption side is shown in Figure 8.

In encryption side, the histogram is plotted for the original PET image, baker key [2 4 2] is applied to an input image and the resultant image is a chaotic baker image, and encrypted image.

In decryption side, histogram is plotted for input image which is equal to the encrypted image, chaotic baker image, and the decrypted image which is equal to the original image. Here, the histogram of the original input image and decrypted image both are same.

The analysis is taken and compared the sample input images which has in Figure 5. The output performance is measured for those images and the measured value is tabulated in Table 1 and plotted in Figure 9 and 10 respectively.

Table 1: Performance Evaluation of hybrid baker map with AES in CBC mode for Ultrasound and PET images

S.No	Parameters	Ultrasound	PET
1.	PSNR (dB)	66.17	59.00
2.	MSE	0.0151	0.0199
3.	Entropy of original image (bits/pixel)	6.9371	5.999
4.	Entropy of encrypted/watermarked image (bits/pixel)	7.9997	7.997
5.	Correlation coefficient	0.0019	0.0152
6.	Embedding rate	0.1	0.1
7.	Time required (sec)	2.572	3.134

Figure 9: Performance of Ultrasound images

Figure 10: Performance of PET images

CONCLUSION

To avoid complexity of work and time, the system access to two messages in the spatial domain and encrypted domain concurrently. These two messages with hash code, pseudo random sequence of bits and authenticity code are embedded to

verify the integrity and authenticity of medical images like Ultrasound images and PET images even if it is encrypted. This system gives an efficient PSNR value of 66.17 dB for ultrasound images and 59.17 dB for PET images. This improved PSNR value represents noise free or error free output image because of its low mean square error value. At the same time the system

gives high entropy and low correlation coefficient value due to the process of baker map preprocessing tool. This system maintains the embedding rate upto 0.1bpp and reduces the processing time to 2.572 sec due to concurrent double watermark.

REFERENCES

- Coatrieux G, Le Guillou C, Cauvin J M, Roux C. Reversible watermarking for knowledge digest embedding and reliability control in medical images. *IEEE Transactions on information technology in biomedicine* 2009; 13:158-165.
- Rajendra Acharya U, Acharya D, Subbanna Bhat P, Niranjana U C. Compact storage of medical images with patient information. *IEEE Transactions on information technology in biomedicine* 2001; 5:320-323.
- Shiguo L, Zhongxuan L, Zhen R, Haila W. Commutative encryption and watermarking in video compression, *IEEE Transactions on Circuits Systems Video Technology* 2007; 17:774-778.
- Chen B, Wornell G W. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on information theory* 2001;47: 1423-1443.
- Al-Qershi O M, Khoo B E. Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. *Journal of Digital Imaging* 2011; 24:114-125.
- Boucherkha S, Benmohamed M. A lossless watermarking based authentication system for medical images. *World Academy of Science and Technology* 2007; 1:20-23.
- Celik M U, Sharma G, Tekalp AM, Saber E. Lossless generalized-LSB data embedding. *IEEE Transactions on image processing* 2005; 14:253-266.
- Chao H M, Hsu C M, Miaou S G. A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. *IEEE Transactions on Information Technology in Biomedicine* 2002; 6:46-53.
- Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, Christian Roux. A Joint Encryption/Watermarking System for verifying the Reliability of Medical Images, *IEEE Transactions on Information Technology in Biomedicine* 2012; 16:891-899.
- Epstein M A, Pasieka M S, Lord W P, Wong S T C, Mankovich N J. Security for the digital information age of medicine: issues, applications, and implementation. *Journal of Digital Imaging* 1998; 11:33-44.
- Giakoumaki, Sotiris Pavlopoulos, Dimitris Koutsouris. Multiple Image Watermarking Applied to Health Information Management. *IEEE Transactions on Information Technology in Biomedicine* 2006; 10:722-732.
- Gouenou Coatrieux, Hui Huang, Huazhong Shu, Limi Luo, Christian Roux. A Watermarking based Medical Image Integrity Control System and an Image Moment Signature for Tampering Characterization. *IEEE Journal of Biomedical and Health Informatics* 2013; 17:1057-1067.
- Mohamed M Abd-Eldayem. A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine. *Elesiver Egyptian Informatics Journal* 2014;14:1-13.
- Mostafa S A K, El- sheimy N, Tolba A S, Abdelkader F M, Elhindy H M. Wavelet packets-based blind watermarking for medical image management. *Journal of Biomedical Engineering* 2010; 4:93-98.
- Ni, Z, Shi, Y Q, Ansari, N, Su, W. Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology* 2006; 16:354-362.
- Ou, Y, Sur, C, Rhee, K H. Region-based selective encryption for medical imaging *Frontiers in Algorithmics*. Springer 2007; 4613:62-73.
- Qingqi Pei, Xiang Wang, Yuan Li, Hui Li. Adaptive Reversible Watermarking with Improved Embedding Capacity. *Elsevier Journal of Systems and Software* 2013; 86:2841-2848.
- Tan, C K, Ng, C, Xu, X, Poh, C L, Guan, Y L, Sheah, K. Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. *Journal of Digital Imaging* 2011; 24:528-540.

Cite this article as:

Amudha K *et al.* Hybrid baker map with AES in Cipher block chaining mode in medical images. *Int. Res. J. Pharm.* 2017;8(4):67-73 <http://dx.doi.org/10.7897/2230-8407.080451>

Source of support: Nil, Conflict of interest: None Declared

Disclaimer: IRJP is solely owned by Moksha Publishing House - A non-profit publishing house, dedicated to publish quality research, while every effort has been taken to verify the accuracy of the content published in our Journal. IRJP cannot accept any responsibility or liability for the site content and articles published. The views expressed in articles by our contributing authors are not necessarily those of IRJP editor or editorial board members.