IJIRSET

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

A Secured Joint Encrypted Watermarking In Medical Image Using Block Cipher Algorithm

V.Amutha[#1], C.T. Vijay Nagaraj[*2]

[#1]PG Scholar, Communication Systems, Mount Zion College of Engineering and Technology, Pudukkottai, Tamil Nadu, India

[*2]Assistant Professor, Department of Electronics and Communication Engineering, Mount Zion College of Engineering and Technology, Pudukkottai, Tamil Nadu, India

ABSTRACT At present year, most of the hospitals and diagnostic centre have exchanging the biomedical information through wireless media. reliability of the information can be verified by adding ownership data as the watermarking and encryption in the original information. In our proposed work, a joint encryption/watermarking system for the purpose of protecting medical image. This system based on approach which combines a substitutive watermarking algorithm with an encryption algorithm, advanced encryption standard (AES) in counter mode. If the watermarking and encryption are conducted jointly at the protection stage, watermark extraction and decryption can be applied independently. The capability of our system to securely make available security attributes in encrypted domains while minimizing the elapsed time. Furthermore, by making use of the AES algorithm in counter (CTR) mode make our compliant with the DICOM (Digital Imaging and Communications in Medicine) standard.

KEY WORDS - Block cipher, cryptography, encryption, medical image security, decryption, watermarking.

I. INTRODUCTION

The rapid evolution of multimedia transmission and bio-medical information through the internet requires elevated level security and authenticity. Watermark is added ownership to increase the level of security and to verify authenticity. Patients' information (Electronic Patient Record), logo of the hospitals or diagnostic centers can be added in the bio-medical data as watermark to prove the intellectual Property rights [1]. Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers [2].
In cryptography, the transmission and sharing of data increases security issues in terms of [3]

1) Confidentiality, which means that only authorized users can access patient data;

2) Availability, which guarantees access to medical information for authorized user only,

3) Reliability, which is based on a) integrity is a proof that the information has not been altered or modified by unauthorized persons;

b) authentication is a proof of the information origins and of its attachment to one patient. Reliable pieces of information can be used confidently by the physician.

Watermarking techniques are suitable for copy right protection. The general process of watermarking is illustrated in Figure 1.The process can be divided into 3 parts, Embedding, Transmission and Extraction.

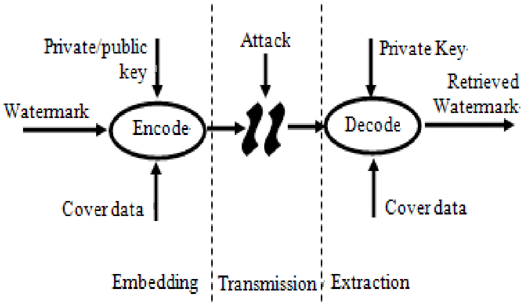


Fig. 1. General process of watermarking System.

In the embedding process, the watermark may be encoded into the cover data using a specific key [4]. This key is used to encrypt the watermark as an additional protection level. The output of the embedding process, the watermarked image, is then transmitted to the recipient. During this transmission process, the watermarked image may be subjected to attacks either deliberately or due to transmission error or noise. Therefore, there is no guarantee that the watermarked image received by the recipient is exactly the same data as that sent by the transmitter. This data nonetheless need to be decoded to extract the watermarked image. The original covered data is needed in the extraction process [1] [4].

II. CRYPTOGRAPHIC PRIMITIVES

The Cryptography plays an important role in the security of data transmission. Basically, there exist two types of encryption algorithms: block cipher algorithms and stream cipher algorithms. Block cipher algorithms, like the AES and the DES, operate on large blocks of plaintext, whereas stream cipher algorithms, like the RC4, manipulate stream of bits/bytes of plaintext [5].

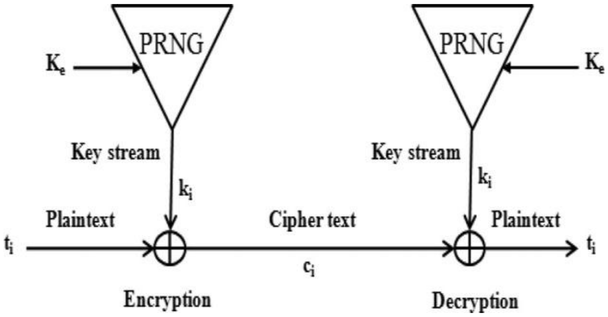


Fig. 2. Encryption/Decryption Process of a Stream Cipher Algorithm

In this paper, it merges a digital watermarking algorithm and an encryption algorithm which can be a block cipher algorithm (AES). In cryptography, the message is usually scrambled and unreadable. However, when the communication happens, it is known or noticed. Although the information is hidden in the cipher, an interception of the message can be damaging, as it still shows that there is communication between the sender and receiver. In contrast, steganography takes a different approach in hiding the evidence that even a communication is taking place. There are two main types of cryptography:

A. **Secret key cryptography** is also known as *symmetric key* cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

B. Public key cryptography, also called *asymmetric encryption*, uses a pair of keys for encryption and decryption. With public key cryptography, keys work decryption.

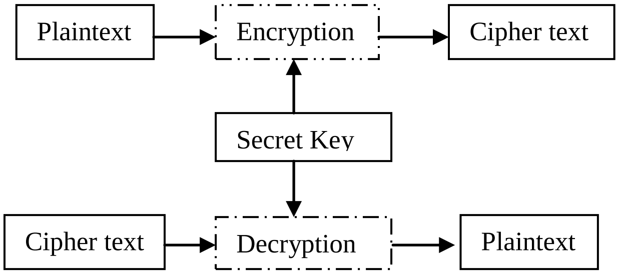


Fig. 3. Encryption and Decryption Process

III. PROPOSED JOINT ENCRYPTION AND WATERMARKING SYSTEM

A. Joint E/W Approach

In our proposed scheme, the Advanced Encryption standard algorithm (AES) used for encrypting the given transmission of data and an medical image. Then digital watermarking technique used for encrypted data was hidden in the transmitted medical image. The both process merged in our system this is called a joint encryption and watermarking system. It is usually required that the watermarked information remains hidden from any unauthorized user (as with data encryption, a secret key is needed to access the watermark content) [7].

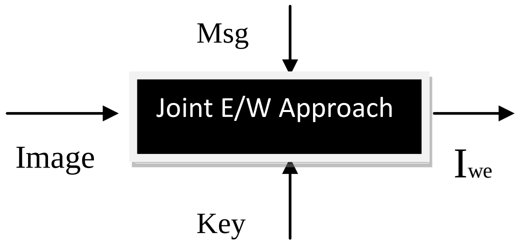


Fig. 4. Architecture of the Proposed Scheme

B. The Advanced Encryption Standard Algorithm

Advanced Encryption Standard (AES) is a very powerful standard block cipher algorithm compared to the data encryption standard (DES) algorithm [8]. The AES is a block cipher, meaning that it operates on an input block of data of a known size and outputs a block of data which is the same size. An input key is also required as input to the AES algorithm. A mode of operation is selected which selects a specific implementation of the AES algorithm. The input blocks and output block data are each a fixed length size of 128 bits. The unencrypted data is referred to as Plaintext, and the encrypted data is referred to as Cipher Text.

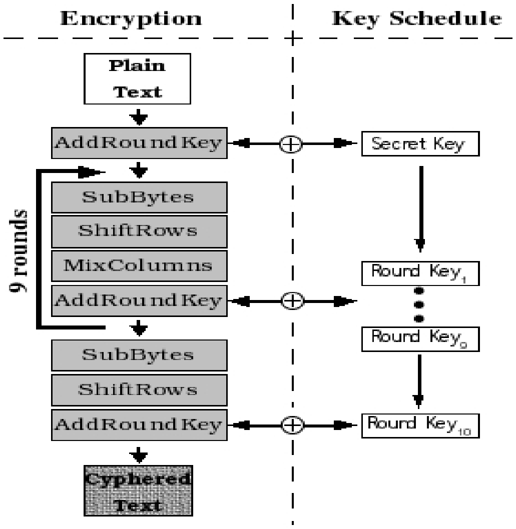


Fig. 5.General Structure of AES Algorithm

The input key can be 128, 192 or 256 bits. The same key is used for both encryption and decryption. In general, the longer the key, the higher the security level obtained with the encryption [8] [9].

The AES encryption algorithm involved four stages. These are as follows,

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

However, the decryption process is not identical to the encryption process. The above four stage of encryption algorithm is reversible. For the sub bytes, shift rows, mix columns stages, an inverse function is used in the decryption algorithm.

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

That Operates by performing a set of steps, for a number of iterations called rounds. The AES algorithm can support several modes such as Electronic Codebook (ECB), Cipher Block Chaining (CBC), Output FeedBack (OFB), Cipher FeedBack (CFB) and Counter (CTR). In CTR mode, each block of plaintext is XORed with an encryption counter. The counter value is incremented to each subsequent block [10].

$$Ci = Pi \bigoplus Ki$$

The plaintext block is XORed with an encryption counter. The counter value is simultaneously incremented to each block. Working with the AES in CTR mode makes our solution transparent or compliant to the (Digital Imaging and Communication in Medicine) DICOM standard. More precisely, if a system is not watermarking interoperable, it will be able to decrypt and access the image if it knows the AES encryption key [3] [11].

C. Watermarking Technique

There are several approaches, methods and techniques have been developed to protect our information during transfer data from source to destination like Cryptography, Steganography and digital image Watermarking. Fundamentally, watermarking can be described as a method for embedding information into another signal [12]. In our proposed system, digital watermarking scheme is implemented with an encryption algorithm for hiding the patient data in an medical image.

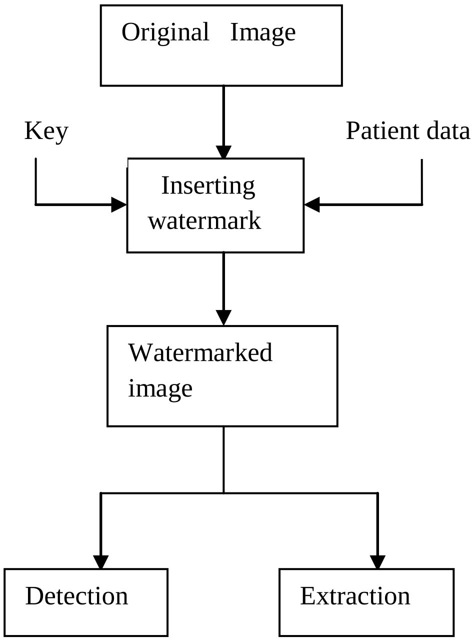


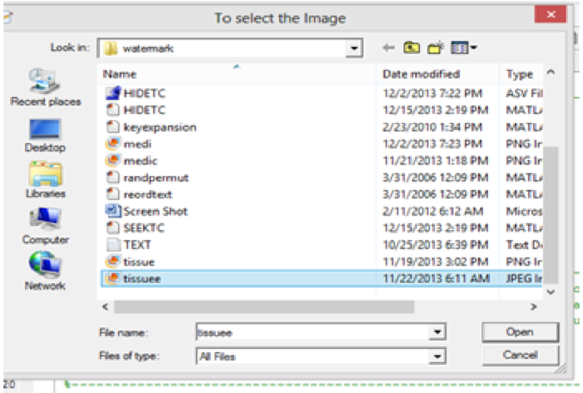
Fig. 6. Scheme of Digital Watermarking

Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection.

The embedded information can be either visible or hidden from the user. A host image used to hide the secret data is called the host image or the carrier image. After embedding the secret data into the host image, the resultant image is called the watermarked image. After that watermarked image the secured encrypted data are decrypted from the encrypted image.

IV. RESUTS AND DISCUSSION

In our proposed scheme, a joint E/W system is to be suitable for real time transmission of images. However, its main advantage is that it gives access to a message in both encrypted and spatial domains. Furthermore, time computation for image decryption remains the same for image encryption. Working with the AES in CTR mode makes our solution transparent or compliant to the DICOM standard. More precisely, if a system is not watermarking interoperable, it will be able to decrypt and access the image if it knows the AES encryption key. The elapsed time was same for both encryption and decryption.



Look in: watermark

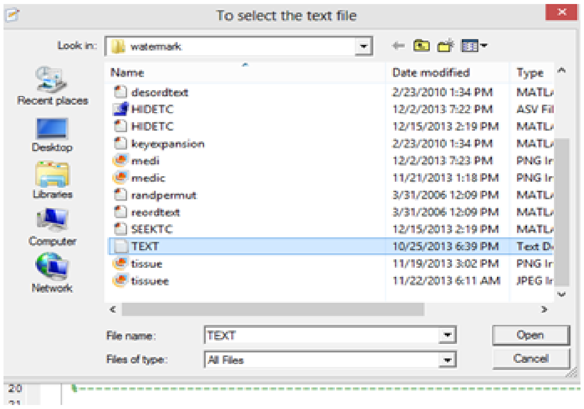
Name	Date modified	Type
HIDETC	12/2/2013 7:22 PM	ASV Fil
HIDETC	12/15/2013 2:19 PM	MATL
keyexpansion	2/23/2010 1:34 PM	MATL
medi	12/2/2013 7:23 PM	PNG Ir
medic	11/21/2013 1:18 PM	PNG Ir
randpermut	3/31/2006 12:09 PM	MATL
reordtext	3/31/2006 12:09 PM	MATL
Screen Shot	2/11/2012 6:12 AM	Micros
SEEKTC	12/15/2013 2:19 PM	MATL
TEXT	10/25/2013 6:39 PM	Text D
tissue	11/19/2013 3:02 PM	PNG Ir
tissuee	11/22/2013 6:11 AM	JPEG Ir

File name: tissuee

Files of type: All Files

Fig. 7. Original Image selection

Fig 7 represents the selecting of medical image for hiding the secret data. In the AES encryption, to convert the original message into coded message i.e., ciphers text and the digital watermarking used to hidden the data inside an image.

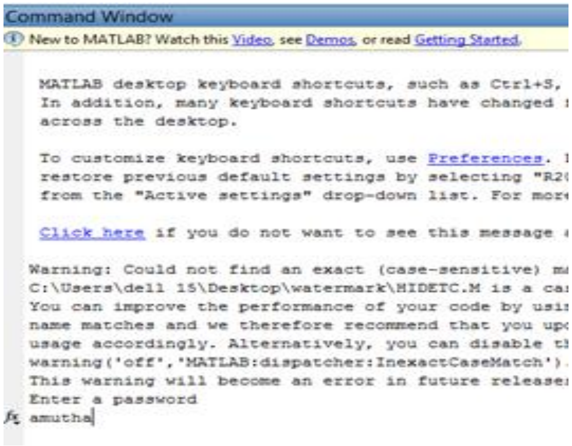


Name	Date modified	Type
desordtext	2/23/2010 1:34 PM	MATL
HIDETC	12/2/2013 7:22 PM	ASV Fil
HIDETC	12/15/2013 2:19 PM	MATL
keyexpansion	2/23/2010 1:34 PM	MATL
medi	12/2/2013 7:23 PM	PNG Ir
medic	11/21/2013 1:18 PM	PNG Ir
randpermut	3/31/2006 12:09 PM	MATL
reordtext	3/31/2006 12:09 PM	MATL
SEEKTC	12/15/2013 2:19 PM	MATL
TEXT	10/25/2013 6:39 PM	Text D
tissue	11/19/2013 3:02 PM	PNG Ir
tissuee	11/22/2013 6:11 AM	JPEG Ir

File name: TEXT
Files of type: All Files

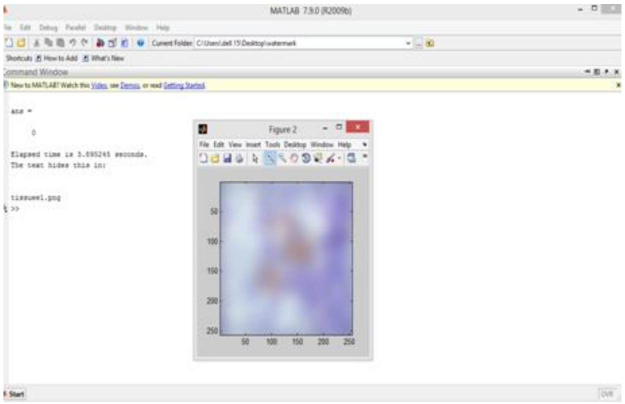
Fig. 8. Hiding Data Selection

Fig. 9. Represents the selection of secret data and this data hide in the previously selected tissue image. It is also depends on the pervious process of joint/encryption and watermarking system. This data was hidden after the encryption. The encryption key for both medical image and data for secure transmission. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. In this process using the advanced encryption standard (AES) expansion key up to 256 key will be used.


Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
  MATLAB desktop keyboard shortcuts, such as Ctrl+S,
  In addition, many keyboard shortcuts have changed
  across the desktop.

  To customize keyboard shortcuts, use Preferences.
  restore previous default settings by selecting "R2
  from the "Active settings" drop-down list. For more

  Click here if you do not want to see this message

Warning: Could not find an exact (case-sensitive) ma
C:\Users\dell 15\Desktop\watermark\HIDETC.M is a ca
You can improve the performance of your code by usi
name matches and we therefore recommend that you up
usage accordingly. Alternatively, you can disable th
warning('off','MATLAB:dispatcher:InexactCaseMatch').
This warning will become an error in future release
Enter a password
amutha
```

Fig. 9. Encryption Key

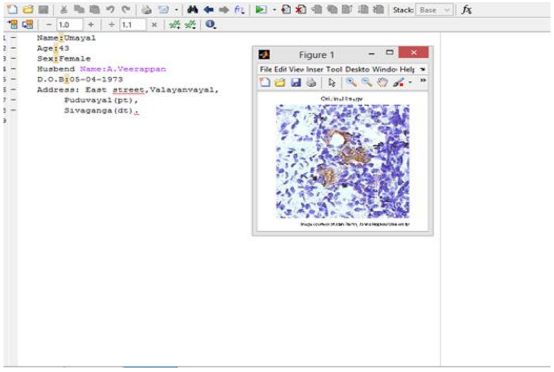

MATLAB 7.9.0 (R2009b)
File Edit Debug Parallel Desktop Window Help
Current Folder: C:\Users\dell 15\Desktop\watermark
Shortcuts How to Add What's New
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
Figure 2
File Edit View Insert Tools Desktop Window Help
50
100
150
200
250
50
100
150
200
250
Start
OVR

```
ans =

     0

Elapsed time is 3.895245 seconds.
The text hides this in:


tissue1.png
>>
```

Fig. 10. Encrypted Medical Image and Data

Figure .10 represents the encrypting of both original medical image and data. Then also calculating the processing time for hiding image and data using joint encryption algorithm (AES in counter mode) and watermarking system. All the above processing performed in transmitter side.

The receiver side, the selecting hidden medical image and data are extracted from the encrypted image using watermark extraction and decryption key. Enter the same encryption key for retrieved medical data. This is called symmetric encryption key because sender and receiver using same key for both encryption and decryption. Figure .11 represent the receiver gets the original image and original data using watermarking extraction and AES decryption technique. This is also reverse process of both watermark embedding and encryption process.



```
Name:Umayal
Age:43
Sex:Female
Husbend Name:A.Veerappan
D.O.B:05-04-1973
Address: East street,Valayanvayal,
     Puduvayal(pt),
     Sivaganga(dt).
```

Fig. 11. Retrieved Original Image and Data

V. CONCLUSION

In this paper, I have proposed a new joint encryption/watermarking system, which guarantees an a priori and a posteriori protection of medical images. It merges the digital watermarking and block cipher algorithm. Our system gives access to verifying the image confidentiality, integrity and reliability even though it is encrypted. The AES in counter (CTR) mode makes our system compliant with the DICOM standard. A simulation result shows the secured transmission of image and data with processing time was low. On the other hand, the execution time for image decryption is not impacted. We have also shown that the way we combine encryption and watermarking does not interfere with the security of the encryption algorithm and that the security of our system depends on the knowledge of the encryption key.

REFERENCES

[1] Nilanjan Dey, Prasenjit Maji, Poulami Das, Shouvik Biswas, "*An Edge Based Blind Watermarking Technique of Medical Images without Devalorizing Diagnostic Parameters*", International Journal of Computer and Communication Engineering, Sep. 2012.

[2] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, "*New Comparative Study Between DES, 3DES and AES within Nine Factors*", Journal of Computing, Vol. 2, no. 3, Mar. 2010.

[3] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic and Christian Roux, "*A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images",* IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 5, sep. 2012

[4] Chunlin Song, Sud Sudirman, Madjid Merabti, "*Recent Advances and Classification of Watermarking Techniques in Digital Images",* International Conference, Oct. 2009.

[5] M.Pitchaiah, Philemon Daniel, Praveen, *"Implementation of Advanced Encryption Standard Algorithm",* International Journal of Scientific & Engineering Research Vol. 3, no. 3, Mar. 2012.

[6] Gurpreet Kaur, Kamaljeet Kaur, *"Digital Watermarking and Other Data Hiding Techniques",* International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Vol. 2, no. 5, Apr. 2013.

[7] G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, *"Reversible watermarking for knowledge digest embedding and reliability control in medical images*," IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 2, pp. 158–165, Mar. 2009.

[8] J.M. Rodrigues, W. Puech and A.G. Bors, "*Selective Encryption of Human Skin in JPEG Images",* IEEE International Conference in Image Processing, Sep. 2005.

[9] Meredith Lucky, VP Sales, *"AES Encryption and CAST's AES IP Cores",* International Conference, Dec. 2008.

[10] David A. McGrew, *"Counter Mode Security: Analysis and Recommendations",* International Conference, Nov. 2002.

[11] W. Pan, G. Coatrieux, N. Cuppens-Boulahia, F. Cuppens, and C. Roux, *"Watermarking to enforce medical image access and usage control policy,"* in Proc. 6th Int. Conf. Signal-Image Technol. Internet-Based Syst., Kuala Lampur, Malaysia, Dec. 2010, pp. 251–260.

[12] Mohamed Radouane, Tarik Boujiha, "*A Method of LSB substitution based on image blocks and maximum entropy*", International Journal of Computer Science Issues, Vol. 10, No 1, Jan. 2013.