

MEDICAL IMAGE SECURITY USING WATERMARKING, PUBLIC-PRIVATE KEYS AND SECRET KEY CIPHERING: A SIMULATION

¹Femi O. Alamu, ²Victoria O. Adedoyin, ³Alice O. Oke,
⁴Halleluyah O. Aworinde and ⁵Awokala J. Adigun

^{1,2,4}Department of Computer Science & Information Technology, Bowen University, Iwo

^{3,5}Department of Computer Science & Engineering, Ladoke Akintola University of
Technology, Ogbomoso

Correspondence: femialamu@gmail.com, awohal@googlemail.com

ABSTRACT

Modern technologies have eased the way for intruders and adversaries to bypass the conventional identity authentication and identification processes; hence security systems have been developed to a great extent for protection of privacy and security of identities. The work therefore, focus on encrypting medical images, which is meant to provide security and privacy, as well as the ability to employ the use of digital watermarking method to enhance the security and privacy level.

In the cause of this work, some encryption algorithms were considered and how such can be incorporated in order to encrypt images and not ignoring their various advantages and disadvantages. Equally, the chosen encryption algorithm was combined with digital watermarking, which involves data hiding. The data hiding method was designed such that the embedding of sensitive personal information in a generic image without any loss of either the embedded or the host information is possible.

The stream cipher algorithm is chosen to encrypt the image because, it proved to be more quick than other encryption algorithms, it is robust to moderate noise like JPEG compression with high quality factor and problem of homogenous zones can be solved.

The experimental results indicate that the encryption algorithm as well as its combination with the digital watermarking outperforms other approaches in terms of payload capacity and marked image quality. Results from the data hiding scheme also show that no major degradation in performance is noticeable compared to the case where no watermarking is needed.

Keywords: Medical Image Security, Watermarking, Encryption, Stream Cipher Algorithm

1. INTRODUCTION

One of the major concerns through-out the world today is to make high quality health care available to all. Traditionally, part of the difficulty in achieving equitable access to health care has been that the provider and the recipient must be physically present in the same place. Recent advances in information and communication technologies have increased the number of ways health care can be delivered to reduce the difficulty of accessing it and this includes Telemedicine, e-health etc.

E-health is a prominent term in healthcare practice supported by electronic processes and communication. It encompasses a range of services or systems that are at the edge of medicine/healthcare and information technology and it provides software solutions for appointment of data scheduling, and patient data in the image (www.fda.gov.com).

Telemedicine therefore, is an integral part of e-health which deals with the use of electronic and communication technologies to provide and support health care when distance separates the participants. (Lacroix et al, 2002) Telemedicine is a focal point where medicine, information and telecommunication technology meet. Infact, it has a great deal of impact on medical imaging in particular and health care delivery in general.

In recent times, the transmission of visual data is a daily routine and it is necessary to find an efficient and secured way to transmit them over networks. When a patient diagnosis in an image form needs to be sent over a network, which could be complex, espionage is a potential risk and real security problem when sending the data could occur. For ethical reasons, medical imagery cannot be sent when such a risk is present, and has to be better protected. Encryption is the best form of protection in this case.

Hence, there is dare need for content protection through encryption with digital watermarking which is meant to secretly embed a message into the data.

2. INFORMATION HIDING

Throughout the ages, various methods have been devised to conceal information in transit. Tactics in previous times ranged from tattooing the message on a shaved head then waiting for the hair to re-grow before sending the message to placing microfiche with the information under the postage stamp on a letter. With the creation of the Internet and other electronic data transmission mediums, steganography or the art of hiding information, has become even more important and common place. (Morkel et al, 2005)

Data hiding in a paper titled Reversible and high capacity data hiding in Medical images was defined as the insertion of a message, also called content, watermark or embedded message, into a host document or cover media. (Fallahpour, et al, 2010)

Medical image data hiding is the process of hiding a set of patient's data into a diagnosis image imperceptibly, such that it does not perceptually distort the image and such that the hidden data can be accurately recovered at the receiver end. Medical information in general is chiefly made up of the results of analyses, clinical, para-clinical examinations, and personal information (Dusserel, 1997).

The number of medical images online is now on the increase and as a result, there is need to ensure the integrity and security of such data. According to Vinay, et al in a paper titled Medical Image Protection by Using Cryptography Data Hiding and Steganography, it has been observed that transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the net as the need for fast and secure diagnosis is vital in the medical world. (Vinay et al, 2012)

3. ENCRYPTION ALGORITHMS

Encryption algorithms can be separated out according to various characteristics: the systems with a secret key and stream cipher (symmetric systems), and those with public and private keys (asymmetric systems). (Diffie, Hellman, 1976; Ducrot, 1996)

The secret key systems are those which allow encryption and decryption with the same key. It goes without saying that the sender and the recipient must beforehand have exchanged the secret of this key, via a secure method of communication. The systems using a public or asymmetric key can overcome this step by using one key to encrypt the data, and another to decrypt it. Each person should possess a pair of keys, one of which is confidential (the private key) and the other known by the world at large (the public key).

4. SECRET KEY SYSTEMS

The secret key systems are the traditional types of block encryption, which allow encryption and decryption with the same key. Examples include:

Data Encryption Standard (DES): The key is a 56-bit number and can be changed at any time. DES algorithm is designed to work with the binary data. DES can encrypt and decrypt 64-bit data blocks with a 56-bit secret key. The DES algorithm is based on 16 rounds, (a collection of stages repeated 16 times) during which a data block of 64 bits is mixed with the key K, which is also encoded on 64 bits. Once the 16 sub-keys have been generated from the secret key, it is possible to cipher (or decipher) a 64-bit block of data.

The major setback of this algorithm is that the length of its key is limited to 64bits. The current performance level of machines in terms of computational time makes the DES breakable.

Advanced Encryption Standard (AES): The number of rounds in the AES algorithm depends upon the size of the key and the size of the data blocks. It is combined with a number of stages, which include: AddRoundKey, SubByte, ShiftRow, MixColumn.

5. ASYMMETRIC BLOCK SYSTEM, RSA

The Rivest, Shamir, and Adleman (RSA) method differs from the symmetric encryption systems in that it uses two different keys for encryption and decryption. The principle of encoding is based on an acquisition of the image followed by a compression then a segmentation in blocks of L pixels (in normal mode $L = 8$ pixels or 64 bits). (Chang, Hwang and Chen, 2001)

Unfortunately, RSA is a very slow algorithm; much slower than any symmetric system, and even more so because the numbers used are very large. Moreover, it is easily breakable today, even for 512 bits³ numbers. It is currently advisable to use keys 1,024 bits long. It is therefore preferable to use it to send a secret key in a secure way, which will allow the message to be decrypted, with AES faster than RSA.

6. ALGORITHM FOR STREAM CIPHERING

With a stream cipher algorithm, it is possible to encrypt each character of the plaintext separately, using an encryption function which varies each time. In general, algorithms for stream cipher are made up of two stages: the generation of a dynamic key (key stream) and the encryption output function using the dynamic key. If the key stream generator produces a series of zeros, the outputted ciphered stream will be identical to the original plain text.

With a stream cipher algorithm, the sender and receiver have to synchronize using the same key at the same position. Synchronous stream ciphers are used in environments where error is common, because they have the advantage of not propagating errors. (Guillem-Lessard, 2002)

7. APPLICATION OF THE ENCRYPTION ALGORITHMS TO MEDICAL IMAGING

In the case of block (DES and AES) encryption, the length of the blocks is fixed, and varies from 64 bits (8 pixels) to 192 bits (24 pixels). From the bi-dimensional information of an image, several pixel grouping solutions are possible. With the aim of withstanding a downstream compression as well as possible, or compressing at the same time as coding, it is useful to group the pixels with their nearest neighbours (in rows, columns, or blocks). Each block of pixels is encrypted separately. The encrypted block obtained will then come to replace the original block in the image.

Also, applying a stream cipher algorithm with a 128-bit key to an image with (396x400 pixels).. Consequently the function generating the dynamic key $g()$ produces a sequence with a large period and good statistical properties.

8. DIGITAL WATERMARKING

Digital watermarking is a type of data hiding or steganography. It entails inserting some data into a digital image, a sound file or a digital video. (IBM System Journal, 1996) A digital watermark is a secret key dependent signal inserted into digital data (images, sound, and texts) and which can be later detected/extracted in order to make an assertion about the data. (Hartung and Kutter, 1999)

The digital watermark is represented as a kind of 'natural' noise. The identification information is encoded into the original un-watermarked data by adding more 'natural' noise and/or rearranging existing noise.

9. DESCRIPTION OF THE COMBINATION OF THE METHODS

Combination of encryption and watermarking in images involves, constructing a new method with encryption algorithm with secret key for the image, with encryption based on public-private key for the secret key and with watermarking method. For example, if a medical doctor M wants to send, by network, a medical image to a specialist S, it should be made in a safe way. To do that, the doctor M can use a fast encryption algorithm with secret key K to cipher the image. In order to transfer K, M can encrypt the key K by using encryption algorithm with public key, like RSA e.g If pub is a public key and priv a private key for RSA, then M possesses the public and private keys pub_M and $priv_M$, and S the public and private keys pub_S and $priv_S$. Firstly, M generates a secret key K for this session and encrypts the image with the stream cipher algorithm

However, for each session, the value of the secret key K must change. Otherwise, if the key has no changing, all the people who have the software can decrypt the images.

10. METHODOLOGY

Previously, before coming up with this work, image is encrypted using the encryption key and the data to hide is embedded into the image using the same encryption key. The user who knows the secret encryption key used can access the image using the same encryption key. In this case, the encrypted key is sent with the encrypted image and in such a case as this, any user can view the encrypted image with that key. By implication, the security provided for the encryption is not handled properly.

To overcome the problems attached to previous systems, an Encryption-Secure Communication using public key and symmetric key was developed to ease the operation.

With this development, the data hiding and image encryption are done by using two different keys i.e. the encryption key and the data hiding key. In this case, the receiver who has the data hiding key and encryption key can retrieve the data embedded and also the original image without viewing or extracting the data embedded in the encrypted image.

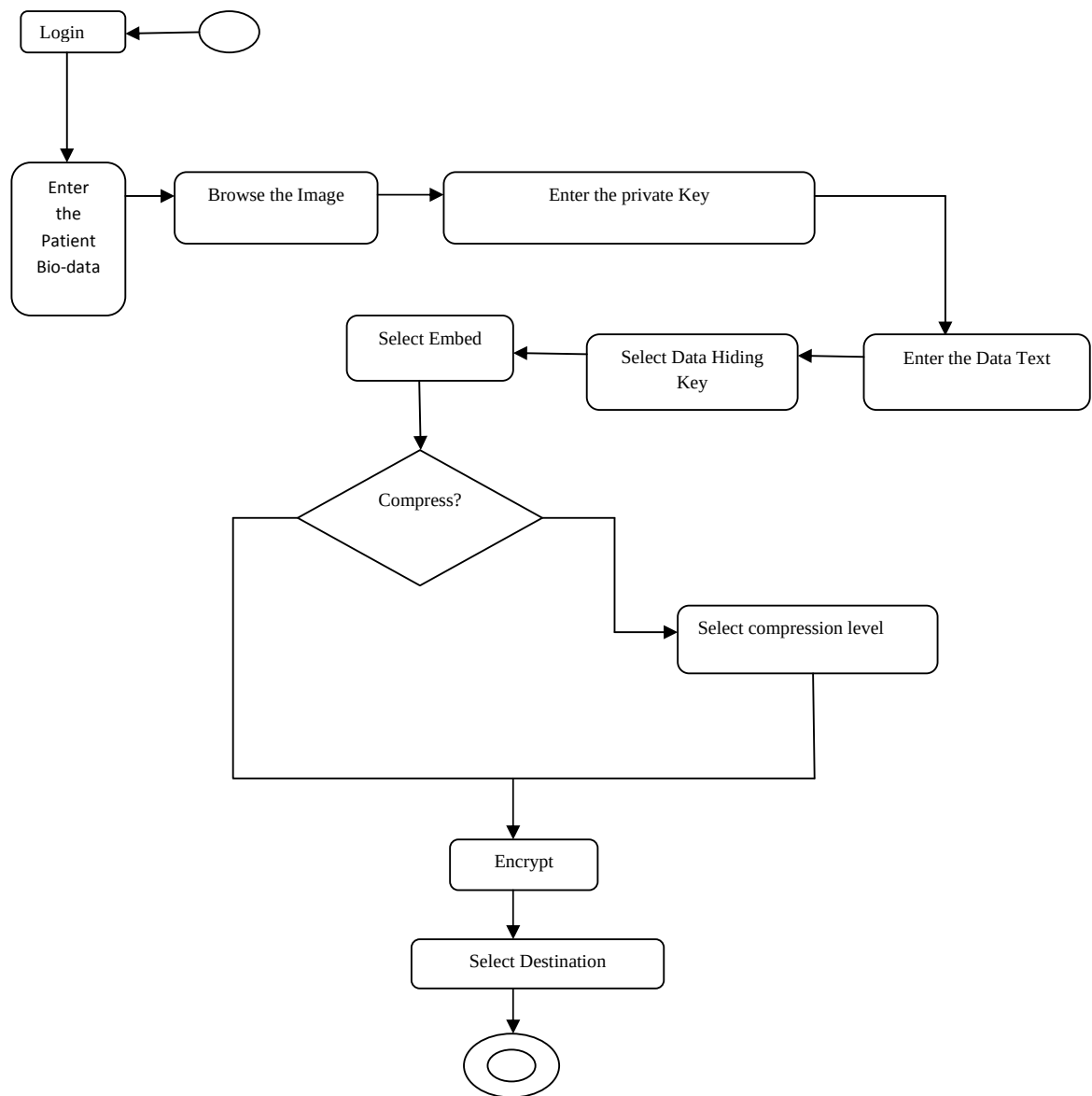


Figure 1: Activity Diagram for Image Encryption with Data Hiding

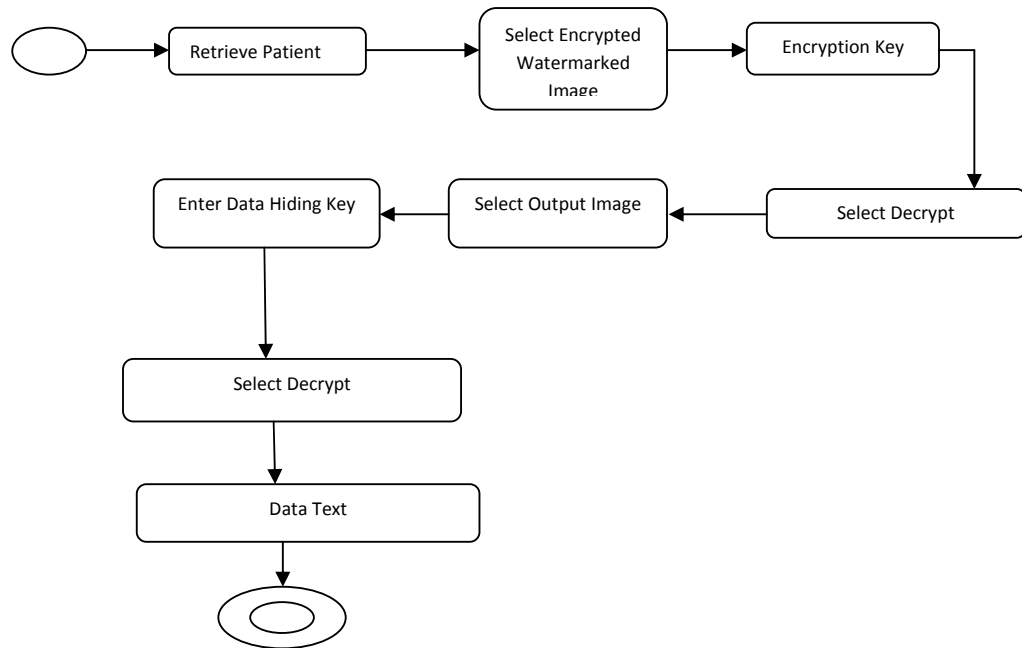


Figure 2: Activity Diagram for Image Decryption with Data Hiding

11. RESULTS

Encrypting the Original Image

This involves browsing for the image that needs to be encrypted from the image directory and supplying a key, which encrypts the image. Illustrations are shown in figure 3 and 4

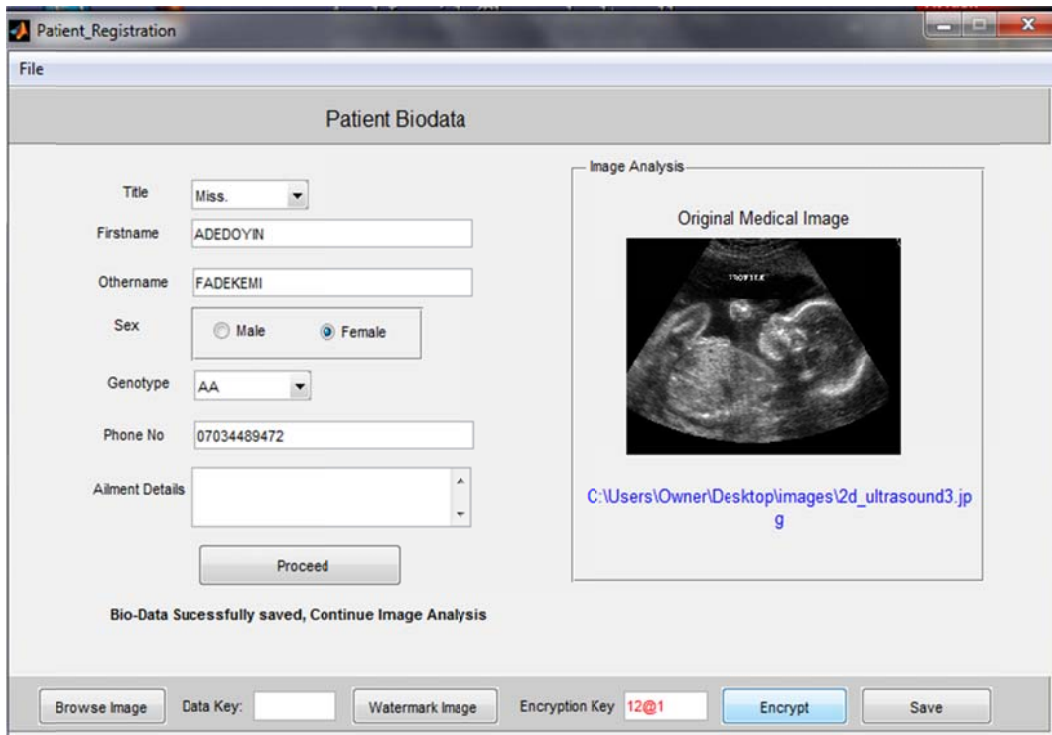


Figure 3: Patient's Biodata with Original Image

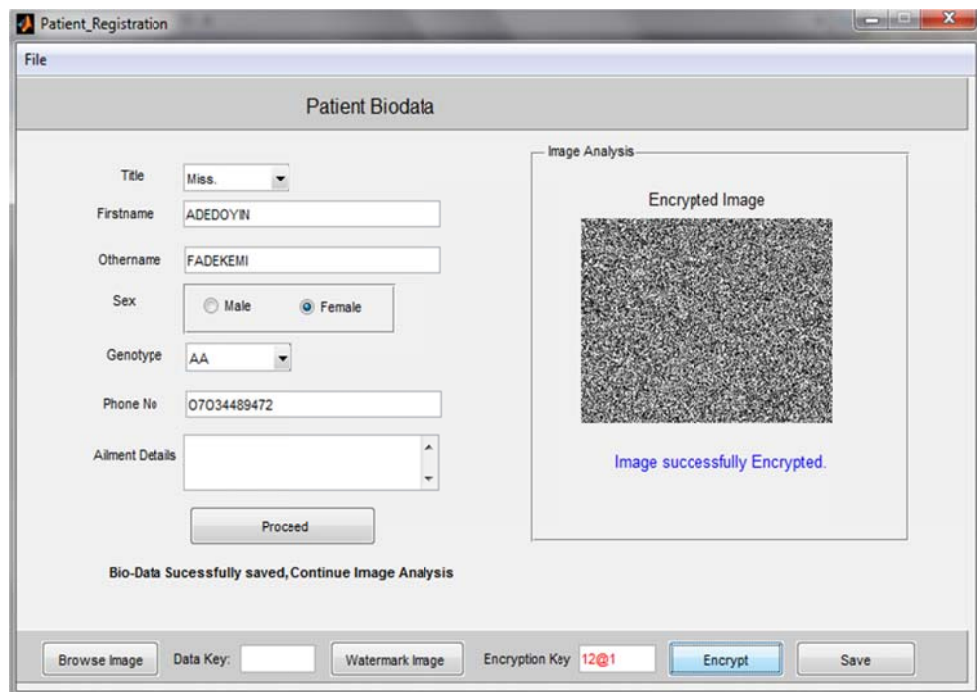


Figure 4: Patient's Biodata with Encrypted Image

Decrypting the Image

In this module, the image encrypted is decrypted by supplying the key that was used in encrypting it. If the recipient has the wrong key, the whole process is cancelled. It is shown in figure 5.

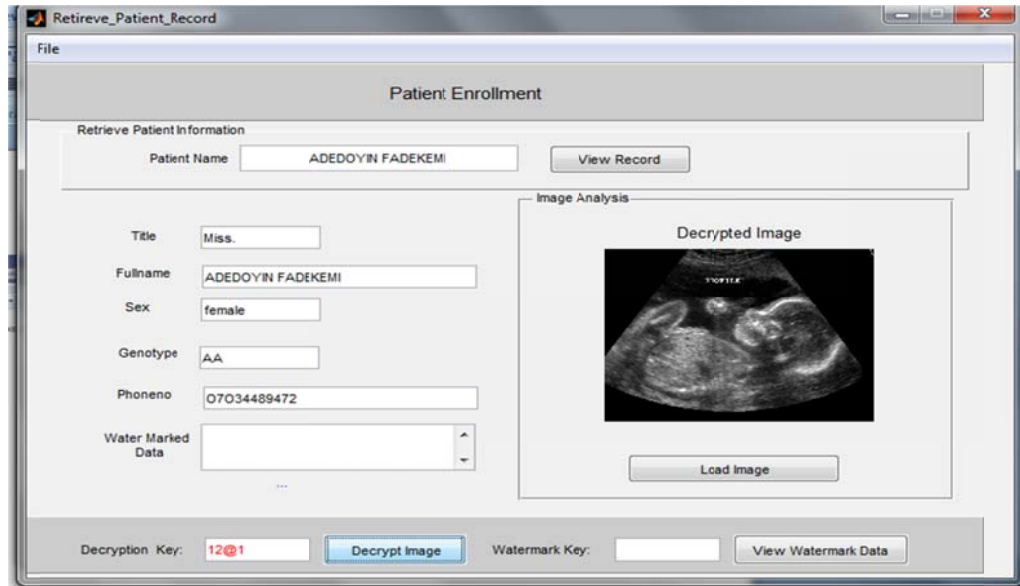


Figure 5: Decrypting Image

Embedding the Data (Watermark)

In this module, the data to be hidden in the image is embedded using the least significant bit. It is given a data hiding key, which has been generated from the algorithm. This embedded data does not affect the quality of the image as shown in figure 6

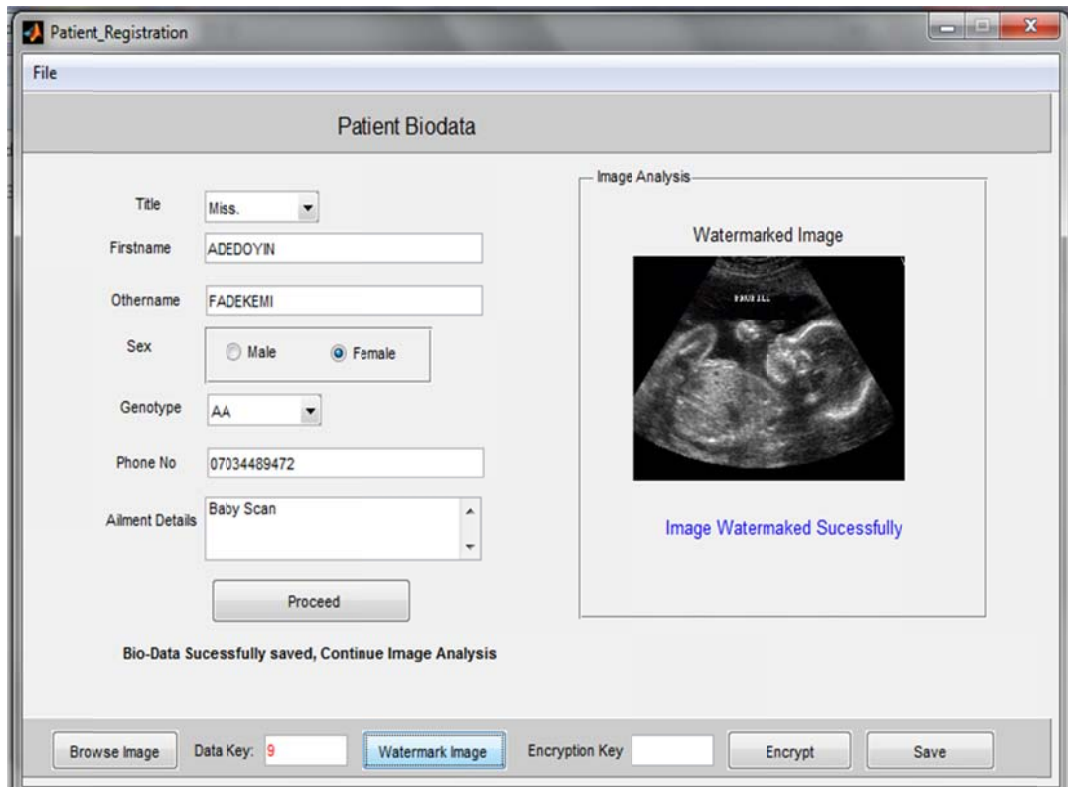


Figure 6: Watermarked Image

Decrypting The Encrypted Image And Watermarked Data

This module captures the decryption of the encrypted watermarked image. If the recipient has the image encryption key, only the image would be decrypted and if its only the data hiding key, only the data would be decrypted. But if he/she has both keys, both would be decrypted. An illustration is shown in figure 7.



Figure 7: Retrieving Patient's Record

12. CONCLUSION

In this work, various encryption algorithms and digital watermarking were considered. Equally, integration of encryption and digital watermarking to encrypt an image and also hide an encrypted data in images were looked into. It consists of image encryption, data hiding, encrypted data hiding and then recovery of the image and data. Encryption of the image and data that is to be hidden is encrypted along with a private key. Then hiding the encrypted data in the image is also given a key called data hiding key. If there is only data hiding key then only the data can be extracted which is in encrypted form along with the original image. If there is only private key then the data alone can be decrypted. When the user has all the keys, it is easy to extract the data and the image without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

The design was able to increase the level of security and ensuring that espionage (obtaining information that is considered confidential) is eliminated in a hospital management system. It is efficient and considered to be very confidential.

REFERENCES

- Amine N. A. and Christine C.M. (2008). Compression of Biomedical Images and Signals, Pp 260.
- Chang C., Hwang M.S. and Chen T.S. (2001). A new encryption algorithm for image cryptosystems, vol 58, Pg 83–91.
- Coatrieux G., Maitre H., Sankur B., Rolland Y., Collorec R. (2000). Relevance of Watermarking in medical imaging, in ITAB'00, Proceedings of ITAB.
- Diffie W., Hellman M.E. (1976). New directions in cryptography, IEEE Transactions on Information Theory, vol. 26, no. 6, Pp 644-654.
- Ducrot H. (1996). Le dossier médical informatisé face à la Loi Française, Informatique et Santé: Aspects Déontologiques, Juridiques et de Santé Publique, vol. 8, Pp 87-96.
- Dworkin M. (2001). SP 800-38A 2001, Recommendation for Block Cipher Modes of Operations.
- Ge X., Jiao R., Tian .H, and Wang J. (2006). Research on Information Hiding, US-China Education Review, USA, Volume 5, No.3, Serial No.18, Pp.77-81.
- Goldreich A b c and Oded (2004). Foundations of cryptography: Volume 2, Basic Applications: Vol. 3. Cambridge University press, Pp 474.
- Guillem-Lessard S. (2002). <http://www.uqtr.ca/~delisle/Crypto>.
- Hartung F. and Kutter M. (1999). Multimedia watermarking techniques, Proceedings of the IEEE, vol. 87, no. 7, Pp 1079–1107.
- Juan RHMA, Perez-Gonzalez F (2000). DCT-Domain Watermarking Techniques for Still images, “Detector Performance Analysis and a New Structure”. IEEE Transactions on Image Processing, vol 9, Pp 55-68.
- Morkel T., Eloff J.H.P, and Olivier M.S (2005). An Overview of Image Steganography, Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), (Published electronically)
- Norcen R., Podesser M., Pommer A., Schmidt H.P., Uhl A. (2003). “Confidential storage and transmission of medical image data”, Computers in Biology and Medicine, vol. 33, Pp 277-292.
- Puech Williams and Coatrieux Gouenou, Hybrid Coding: Encryption-watermarking-compression for Medical Information Security, Chapter 10.
- Puech W., Rodrigues J.M., Develay-Morice J.E. (2006). Transfert sécurisé d'images médicales par codage conjoint : cryptage sélectif par AES en mode par flot et compression JPEG, Traitement du signal (TS), numéro spécial Traitement du signal appliqué à la cancérologie, vol. 23, no. 5.
- Rodrigues J.M., Puech W., Bors A.G. (2006). A selective encryption for heterogenous color JPEG images based on VLC and AES stream cipher.

Said A. (2005). Measuring the strength of partial encryption scheme, IEEE International Conference in Image Processing, vol. 2, Pp. 1126-1129.

Scheier B. (1995). Applied cryptography. Wiley, New York, USA.

<http://www.fda.gov.com>