2015 15th International Conference on Computational Science and Its Applications

A Security Technique for Authentication and Security of Medical Images in Health Information Systems

Quist-Aphetsi Kester[123], Laurent Nana[2], Anca Christine Pascu[2], Sophie Gire[2],Jojo M. Eghan[3], Nii Narku Quaynor[3]
[1]Faculty of Informatics, Ghana Technology University College, Accra, Ghana
kquist-aphetsi@gtuc.edu.gh / kquist@ieee.org
[2]Lab-STICC (UMR CNRS 6285), European University of Brittany, University of Brest, France
[3]Department of Computer Science and Information Technology, University of Cape Coast, Cape Coast, Ghana

***Abstract*— Medical images stored in health information systems, cloud or other systems are of key importance. Privacy and security needs to be guaranteed for such images through encryption and authentication processes. Encrypted and watermarked images in this domain needed to be reversible so that the plain image operated on in the encryption and watermarking process can be fully recoverable due to the sensitivity of the data conveyed in medical images. In this paper, we proposed a fully recoverable encrypted and watermarked image processing technique for the security of medical images in health information systems. The approach is used to authenticate and secure the medical images. Our results showed to be very effective and reliable for fully recoverable images.**

Keywords- health information systems, security, medical images, authentication, recoverable.

I. INTRODUCTION

Health information systems forms a critical parts of one's countries information technology infrastructure due to the sensitivity and nature of data processed over time with regards treatment history, medical records etc. this huge amount of data stored over time can reflect on progress of patients, resistance and adoptability of human to drugs over time and genetic links to causes of diseases over time. Medical imaging forms the dominant part of a health infrastructure. With today's advancement in health systems, remote access to hospital data and cloud storage of health data and imaging data is a key to effective health delivery. The critical nature of health services and the advantages and opportunities provided by software applications makes it possible for health care delivery to be done with more efficiency and timeliness. Efficiency in the sense that the organization of medical records and easy access to records in less time is a milestone in the heath care sector and further advancement in medical technologies for surgical operations guided by sensors and artificial intelligence, more advance technological diagnostic tools for pre medical analysis and examination, better imaging technology for signal processing and vision of internal body systems impacted positively on the health sector. Collaborative real-time information systems for medical practitioners in real-time surgical operations are revolutionizing how health care services are delivered around the globe. Information retrieval and data mining approaches in health care etc have made understanding of causes and treatment more comprehensive as well understanding the effect of administration of adhesive drug on patience and also aid in easy determination of outbreak of diseases through reports at hospitals. This makes Information systems an integral part of cyber critical systems in today's cyber space. These benefits of health systems make it easy for a timely and effective provision of healthcare services.

Security breach of health information system can be very catastrophic to both the host and the clients. There has been a high increase of malicious activities on cyber critical infrastructure and the health sector was no exception, this pose serious threat data residing on such information systems. Migration of health data to third party for management in a private, public or hybrid cloud can pose a lot of challenges to the safety and security data stored in the cloud. Privacy is a key issue when it comes to medical issues in the case of patient and health practitioner relationship. Access control is fundamental to security of data in the clouds but when it comes to data security on file servers and in the cloud, little is left to the client to have control over such approach. Most medical data are in imaging formats and breach in the cloud could expose such data to breach privacy. Hence rigorous security approaches are reacquired in securing medical image data in the cloud and for health information systems. Authentication approaches are highly required as well as data confidentiality. But these approaches of securing medical images have to be fast, reversible and achieve full recoverability of data during the entire process of the processing of the image. This is as a result of the sensitivity nature of the image data and the importance of the information conveyed by the data in the image and hence a loss of data values in the process will pose a lot of problem.

In providing solution to part of the challenges faced in health information systems with regards to data security, we proposed an approach for the security and safety of medical images. In our approach, encrypted and watermarked images can be fully recoverable to meet the demand of the sensitivity of the information conveyed in medical images. It is also effective for tamper detection as well as providing authentication and confidentiality for the medical images. This makes contents stored in such Information infrastructure more secured. The paper has the following structure; section II Related works, section III is Methodology, section IV Results and analysis, and section V concluded the paper.

978-1-4673-7367-8/15 $31.00 © 2015 IEEE
DOI 10.1109/ICCSA.2015.8

II. LITERATURE REVIEW

The current trend of medical image transmission trough the wire network and wireless network is more and more increasing as telemedicine adopt more technology to achieve effective service delivery. Usman, K. et al in their work of medical image encryption based on pixel arrangement and random permutation for transmission security investigated on the utilization pixels arrangement and random permutation to encrypt medical image for transmission security. They engaged a random permutation proceeded by a simple pixels arrangement and fulfilled a high computation speed, and a long permutation key was inherited from the big image size in their process which had resistivity against the brute-force attack [1]. Abokhdair, N.O et al in their work of Integration of chaotic map and confusion technique for color medical image encryption, proposed algorithm based on combination of scrambling and confusion processes. 2D lower triangular map used for scrambling the addresses of image pixels, and the proposed propeller algorithm was used to confuse the gray values of image pixels. Their method also was resistive to brute force attack [2]. Yicong Zhou et al in their work, "a lossless encryption method for medical images using edge maps", showed a new lossless approach, called EdgeCrypt, to encrypt medical images using the information contained within an edge map. Their algorithm can also be applied to grayscale images or color images [3]. Below is one of the results obtained from their work.

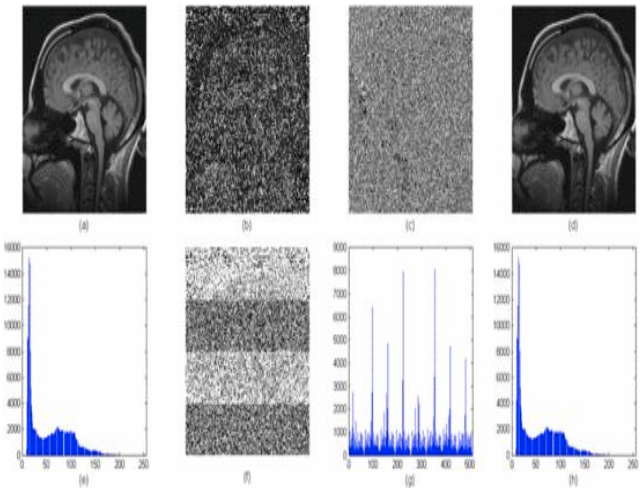


Figure 1. The proposed system's architecture.MRI image encryption. (a) The original MRI image; (b) The edge map obtained by Sobel edge detector with threshold 0.5; (c) The encrypted MRI image, (d) The reconstructed MRI image; (e) Histogram of the original MRI image; (f) The encrypted edge map, x_{0}=0.6 , r=3.65 ; (g) Histogram of the encrypted MRI image; (h) Histogram of the reconstructed MRI image.

There have been other works such as Transmission and storage of medical images with patient information" by R. Acharya U, P et al [4], "Chaos-Based Medical Image Encryption Using Symmetric Cryptography" by M. Ashtiyaniet [5]. etc. Our approach is discussed in the following section.

III. METHODOLOGY

Medical images stored in health information systems carry vital information about patients. The privacy and security of the information carried by the image is very important when it comes to patient information. Hence confidentiality is a key as well authenticity of the image. Most medical facilities store this information of on file servers without encrypting them. Back door access to these images will violate the privacy of patients and wrong processing of a specific image for different patient will further affect the integrity of the medical institution. To solve this problem, we propose a security system in which we have a fully recoverable and reversible process to authenticate and secure medical images in health information systems. The figure below represents the system, security server, which renders such services to its users.

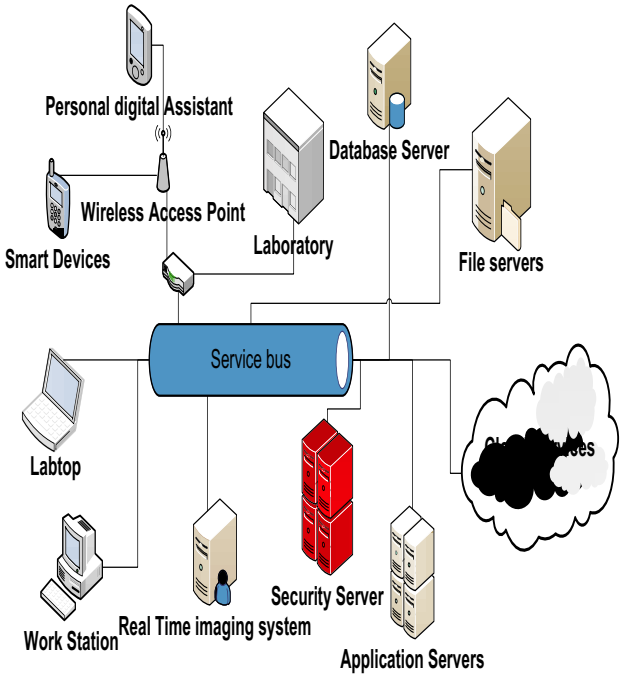


Figure 2. The proposed system's architecture.

With our proposed system, the security server has an application service system that renders confidentiality and authentication services for clients of the system. The security process is a symmetric encryption and decryption service as well as the watermarking for authentication. Disparate devices such as PDAs, PC, etc can communicate via the same service bus to access medical data such as x-ray image data, ultra sound scan documents etc. Any request made by an application with regards to medical images will have services rendered to it via an abstraction level to that application. This means that data storage in file servers, in databases and in cloud will have to transact activities through the security server. With such an implementation, back door access o such data will render such files meaningless.

The encryption process is symmetric and uses client's authentication systems to grant access but uses patients' unique information in the encryption and watermarking of the medical images.

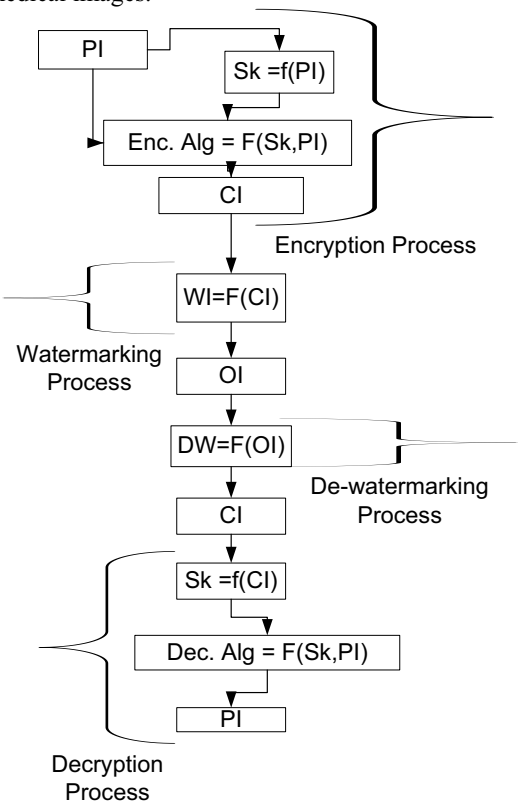


Figure 3. Summary of the process.

In figure above the variables are as follows,
PI=plain Image
Sk=symmetric key
Enc. Alg=Encryption Algorithm
CI=Ciphered Image
WI=Watermarked Image
OI=Final Output Image
DW=De-watermarked Image
Dec. Alg=Decryption Algorithm

A. The Encryption process

a) Import data from image and create an image graphics object by interpreting each element in a matrix.

b) Get the size of r as [c, p]

c) Get the Entropy of the plain Image

d) Get the mean of the plain Image

e) Compute the shared secret from the image

f) Engage SK for g) to q) using secret key value

g) Extract the red component as 'r'

h) Extract the green component as 'g'

i) Extract the blue component as 'b'

j) Let r =Transpose of r

k) Let g =Transpose of g

l) Let b =Transpose of b

m) Reshape r into (r, c, p)

n) Reshape g into (g, c, and p)

o) Reshape b into (b, c, and p)

p) Concatenate the arrays r, g, b into the same dimension of 'r' or 'g' or 'b' of the original image.

q) Finally the data will be converted into an image format to get the encrypted image.

The inverse of the algorithm will decrypt the encrypted image back into the plain image.

The secret key is obtained as follows:

$Sk = [(c \times p) + |(He \times 10^3)| + |(\quad \bar{x} = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \quad)|] \bmod p$

Where c, p are dimension of the image and He is the entropy value of the image and *x* bar is the arithmetic mean for all the pixels in the image.

B. The watremarking process

The watermarking data was applied throughout one channel of the ciphered image. For this work, the R channel was chosen for the procedure. Spatial watermarking approach was chosen but implement by using pixel ciphering tecknic.

Let (:,:,1)=size of R be mxn[row, column]

size (R) = R (m x n)

rij= r=CI (m, n, 1)

Embedding the data into CI

d=Aij, where d is the data to be embedded

$x \in Aij : [a, b]=\{x \in I: a \leq x \geq b\}$ where a=0 and b=255

Let the size of d be [c1, p1] =size (d);

Let λ=xi : x i$\in$ I: $0 \leq x \geq \infty$;

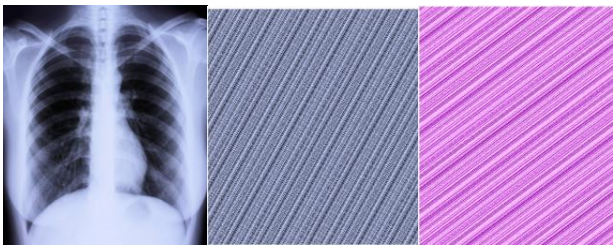
Let η=xi : x i$\in$ I: $0 \leq x \geq \infty$;

```
for i=1:1:c1
    for j=1:1:p1
     r(i,j)=(Aij+ r(i,j)) mod 256;
   end
end
```

The implantation of the approaches was done using MATLAB. The images were encrypted and the results were analyzed below.

IV. Analysis and Results

Three samples of medical images were encrypted by the algorithm using MATLAB and the results are below. The RGB graphs from figure 5 to 9 were plotted using the first 10000 pixel values of both plain and ciphered images.



a) Plain image b) Ciphered Image c) Watermarked Image

Figure 4. X-ray Image of the ribs

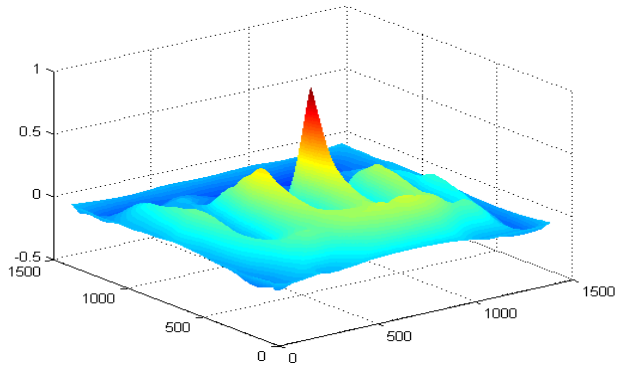


Figure 5. The graph of the normalized cross-correlation of the matrices of the plain image of the X-ray Image

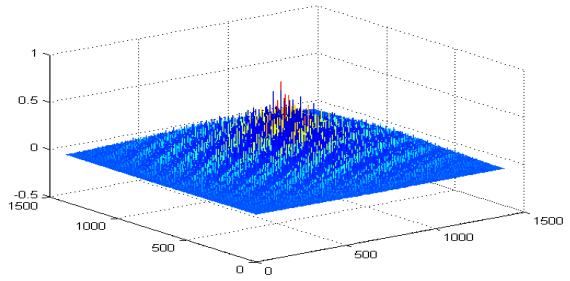


Figure 6. The graph of the normalized cross-correlation of the matrices of the ciphered image of the X-ray Image

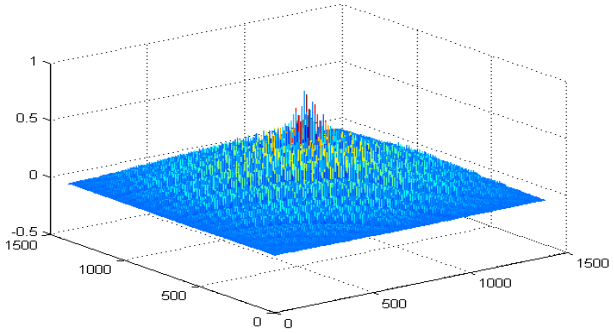
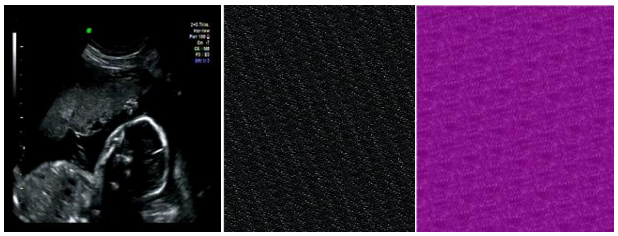


Figure 7. The graph of the normalized cross-correlation of the matrices of the watermarked image of the X-ray Image



a) Plain image b) Ciphered Image c) Watermarked Image

Figure 8. Ultrasound Image of the womb

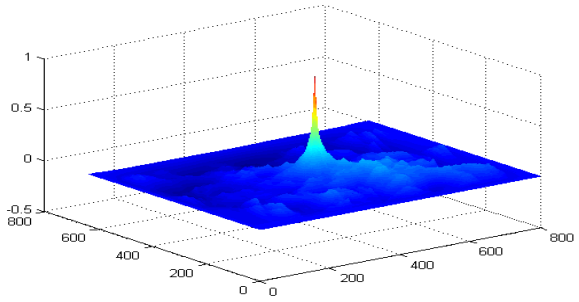


Figure 9. The graph of the normalized cross-correlation of the matrices of the plain image of the Ultrasound Image

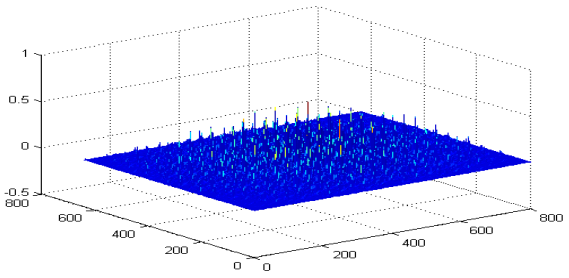


Figure 10. The graph of the normalized cross-correlation of the matrices of the ciphered image of the Ultrasound Image

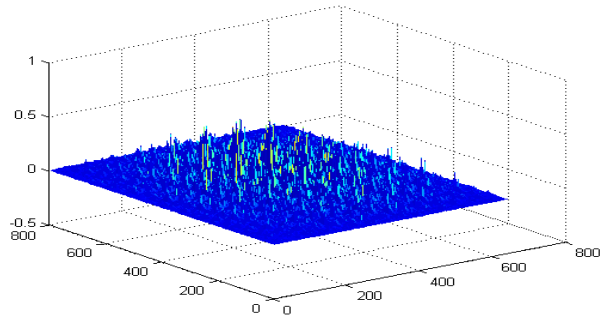
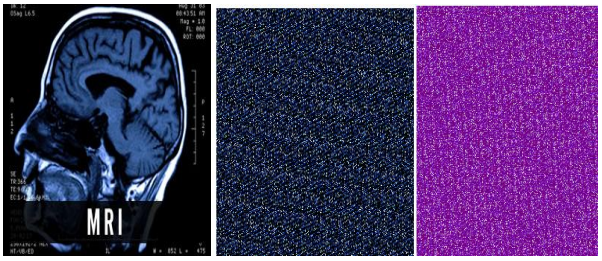


Figure 11. The graph of the normalized cross-correlation of the matrices of the watermarked image of the Ultrasound Image



a) Plain image b) Ciphered Image c) Watermarked Image

Figure 12. Magnetic Resonance Imaging of the brain

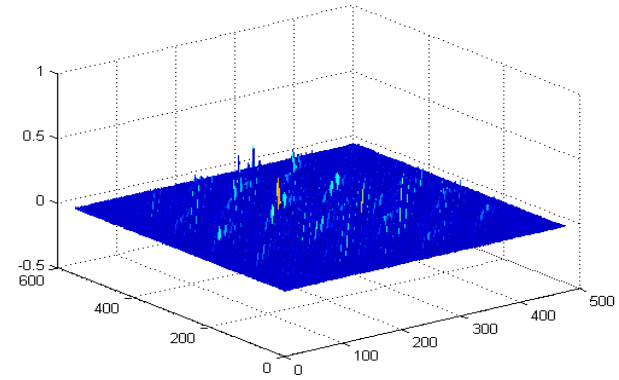


Figure 13. The graph of the normalized cross-correlation of the matrices of the plain image of the MRI Image

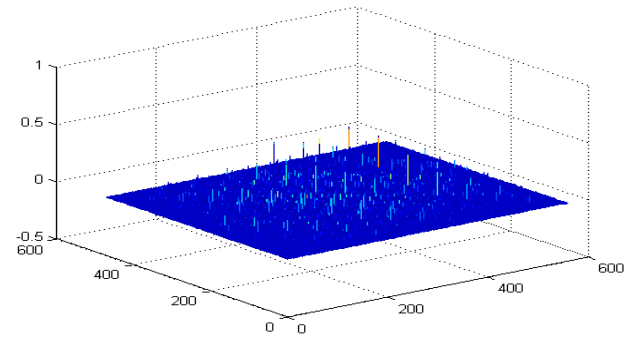


Figure 14. The graph of the normalized cross-correlation of the matrices of the ciphered image of the MRI Image

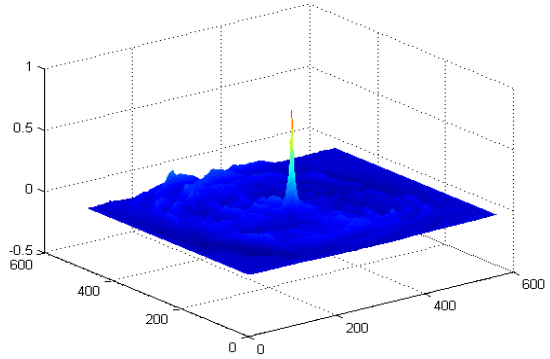


Figure 15. The graph of the normalized cross-correlation of the matrices of the watermarked image of the MRI Image

TTABLE 1: ANALYSIS OF PLAIN, CIPHERD, AND WATERMARKED IMAGE.

	Entropy(p)	*Arithmetic mean(m)*
XPI	7.1726	143.5284
XEI	7.1726	143.5284
XWI	5.6507	195.9617
UPI	3.7603	18.5810
UEI	3.7603	18.5810
UWI	4.5355	97.8913
MPI	4.6894	39.0415
MEI	4.6894	39.0415
MWI	4.9358	112.6761

From the table,
XPI=X-ray plain image
XEI=X-ray encrypted image
XWI=X-ray watermarked image
UPI=Ultrasound plain image
UEI= Ultrasound encrypted image
UWI= Ultrasound watermarked image
MPI= Magnetic Resonance Imaging Plain Image
MEI= Magnetic Resonance Imaging encrypted image
MWI Magnetic Resonance Imaging watermarked image

V. CONCLUSION

Our proposed work was resistive against statistical and brute force attacks. The encryption process was effective for all the images and there was no pixel expansion at the end of the process. The entropy and mean values for the images in were computed. The total entropy and the mean of the plain images never changed for all the ciphered images and the plain images. That is the average total pixel before encryption was the same as the average total pixel after encryption. But there was a change in pixel value during the watermarking process.

Acknowledgments. This work was supported by Lab-STICC (UMR CNRS 6285) at UBO France, AWBC Canada, Ambassade de France-Institut Français-Ghana and the DCSIT-UCC, and also Dominique Sotteau (formerly directeur de recherche, Centre national de la recherche scientifique (CNRS) in France and head of international

relations, Institut national de recherche en informatique et automatique, INRIA) and currently the Scientific counselor of AWBC.

REFERENCES

[1] Usman, K.; Juzoji, H.; Nakajima, I.; Soegidjoko, S.; Ramdhani, M.; Hori, T.; Igi, S., "Medical Image Encryption Based on Pixel Arrangement and Random Permutation for Transmission Security," e-Health Networking, Application and Services, 2007 9th International Conference on , vol., no., pp.244,247, 19-22 June 2007

[2] Abokhdair, N.O.; Manaf, A.B.A.; Zamani, M., "Integration of chaotic map and confusion technique for color medical image encryption," Digital Content, Multimedia Technology and its Applications (IDC), 2010 6th International Conference on , vol., no., pp.20,23, 16-18 Aug. 2010

[3] Yicong Zhou; Panetta, K.; Agaian, S., "A lossless encryption method for medical images using edge maps," Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE , vol., no., pp.3707,3710, 3-6 Sept. 2009

[4] . R. Acharya U, P. Subbanna Bhat, S. Kumar, L. C. Min, "Transmission and storage of medical images with patient information", Computers in Biology and Medicine, vol. 33, no.4, pp.303-310, 2003

[5] M. Ashtiyani, P. M. Birgani, H. M. Hosseini, "Chaos-Based Medical Image Encryption Using Symmetric Cryptography", Information and Communication Technologies: From Theory to Applications 2008. ICTTA 2008. 3rd International Conference on, pp.1-5