

Implementation of RSA Algorithm for CIPHERING Medical Imaging

Anuradha Goswami¹, Associate Prof. Sarika Khandelwal²

¹M.Tech. Student, GITS, Udaipur, anugoswami.goswami@gmail.com, 8058168580

²Dept. of CSE, Geetanjali Institute of Technical Studies, Udaipur. sarikakhandelwal@gmail.com, 7665025000

Abstract--In this paper we will present software designed for remote visualization of medical images with data security transfer. This interface is implemented under MATLAB environment. The implementation of the image cryptography system uses the RSA algorithm with 64 bits private key length. The transfer of images in a secure way for medical diagnosis is insured by generating a watermarked key to encrypt the original image. More, we introduced a comparison study between the obtained performances and those computed with other algorithms such as DES and IDEA.

Keywords: RSA, DES, Image Processing.

1. INTRODUCTION

Nowadays, the data can undergo grave modifications (access to the credit cards, the transactions in e-commerce, espionage of the secret information in military domain) especially through transmissions on the internet. Where from, it is necessary to look a robust method to secure the data [1]. The encoding (ciphering) can bring solutions of this problem much more than the watermarking due to difficulties to break the encoding key. It is in this context that is situated the objective of this work which is interested in the study of an asymmetric encoding method applied for medical images by using the RSA algorithm. The objective is also to decipher it even in the presence of various types of attacks [7].

Indeed, the university hospital centers uses and exchange several sizes and formats of images relative to patients whose contents can possess confidential information, whether it is for the level diagnosis or at the personal level. Especially since these given and images can be remotely exchanged if the centres are interconnected by a network LAN

2. Cryptography Principle

The current ciphering techniques use algorithms with symmetric or asymmetric keys [6].

Among the most common we can quote the encoding of Vigenère in a single key, the symmetric algorithm DES with secret keys and the algorithm RSA with public and private keys. The algorithm RSA, at present is the most successful use for ciphering keys and passwords or counts. The key long varies from 64 to 1024 bits [1]. It has the advantage to be strong in the break if the key is rather long and on the other hand, it does not need to pass on the key deprived via the network to the receiver. 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).

Then every block of quantified data is coded by the public key (e, n) of the transmitter according to the algorithm of figure 1. At the level of the receiver, the deciphering is made by the private key (d, n) [[2, 3].

3. Results and developed interface

We developed under Matlab an interface in which we implemented the algorithm RSA as well as the module of treatment and compression of image. The image is compressed first of all according to the JPEG standard by DCT [4]. The encoding is made in the field of transformed on blocks of 8×8 . Only the coefficient BF will be taken into account to relieve the time of encoding-deciphering and decrease the image size.

At present, we replace the compression DCT method by the wavelets by computing the coefficients (L, H) which will be soft threshold than quantified and coded. The results can end in results (profits) better than those obtained with the DCT. The results are illustrated in figures 3 to 6 with $L=8 \times 8$ and $N=64$.

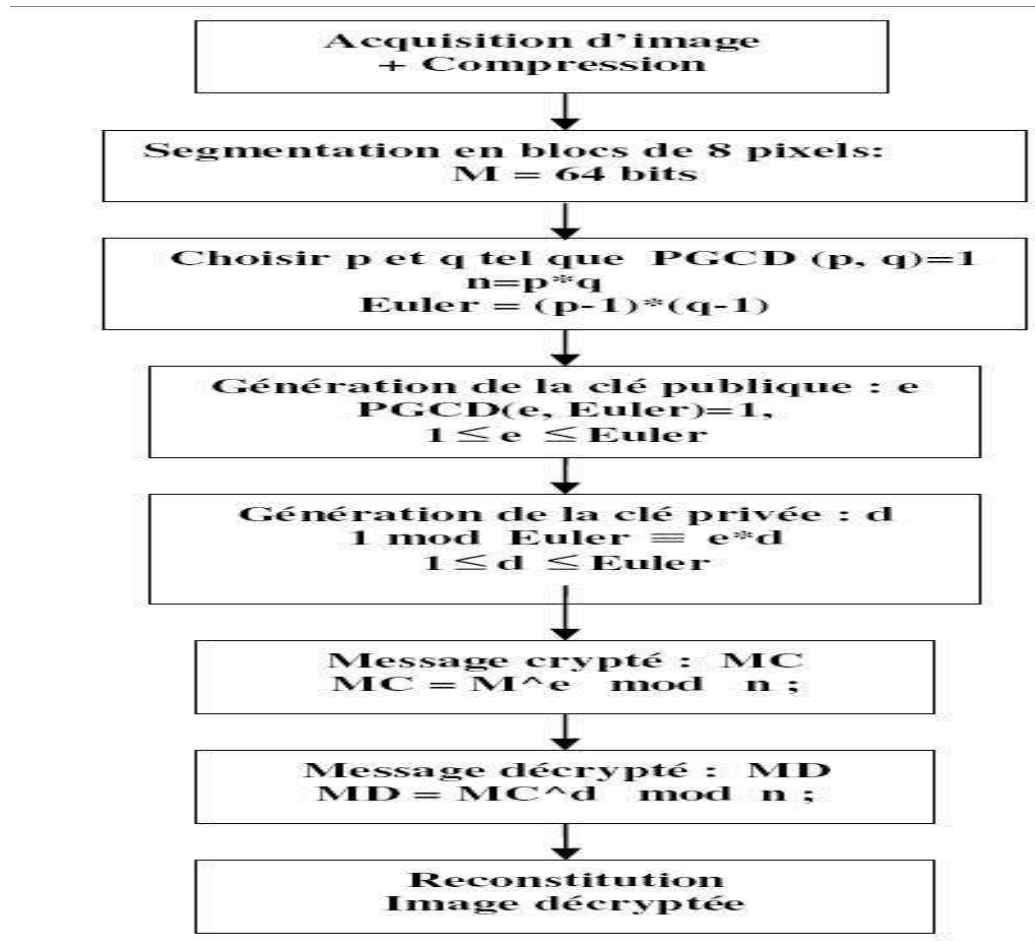


Fig 1 : RSA Algorithm


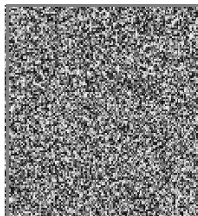


Original Image	Ciphered Image	Deciphered Image	Deciphering error
			

Fig 2: Original and Ciphered images

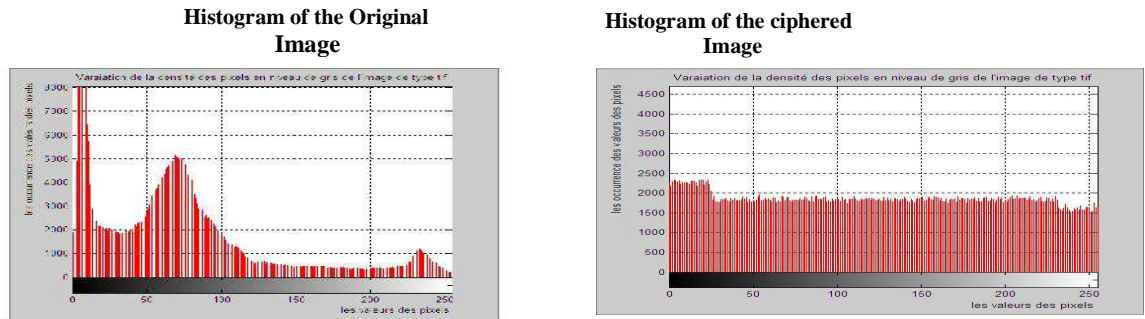


Fig 3: Histogram of the original and ciphered images

Furthermore, we studied the effect of the size of the block L and the key length on the quality of the coded and deciphered image. In the third stage, simulations are made to test the robustness of the

algorithm used according to various types of attack in particular during the transmission [8].

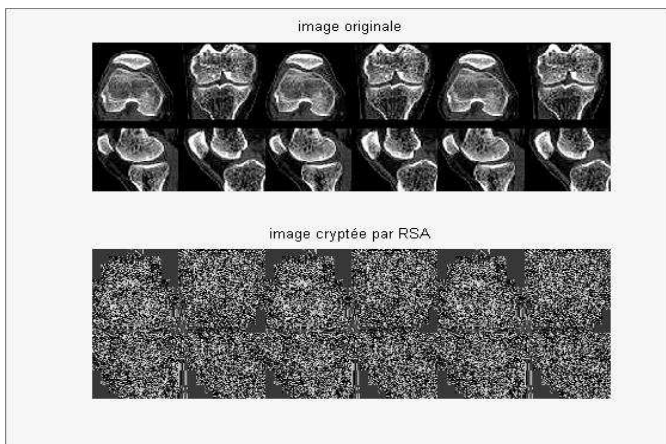


Fig 4: Original and ciphered images for a bloc (L=6 pixels)

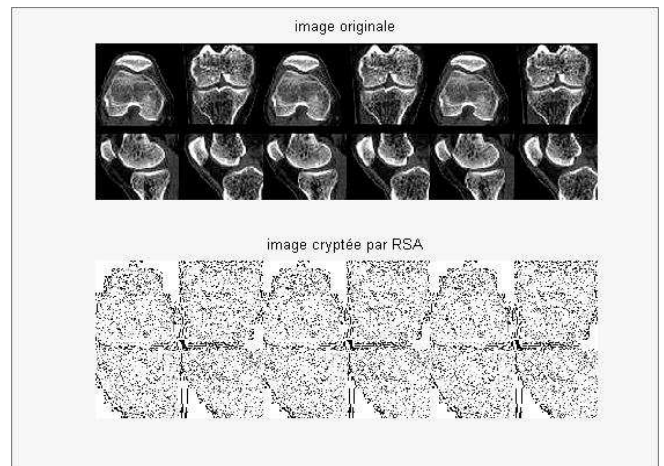


Fig 5: Original and ciphered images for a bloc (L=8 pixels)

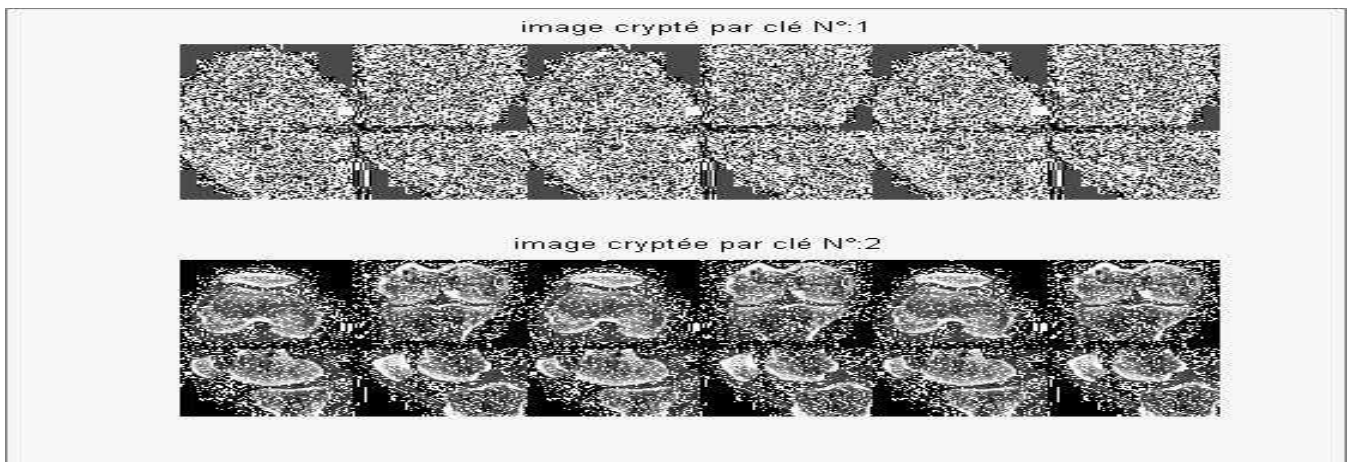


Fig 6: Ciphered images for two distinct keys

Figures 7 and 8 represent the computing times in function of the segmental length L of the image and the ciphering length key.

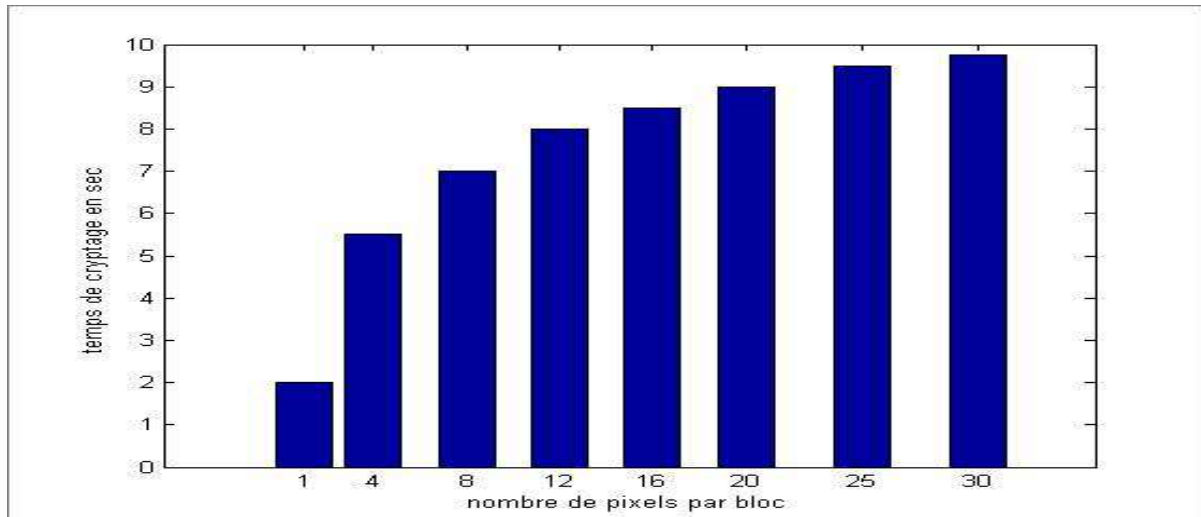


Fig 7: Ciphering time vs. Key length

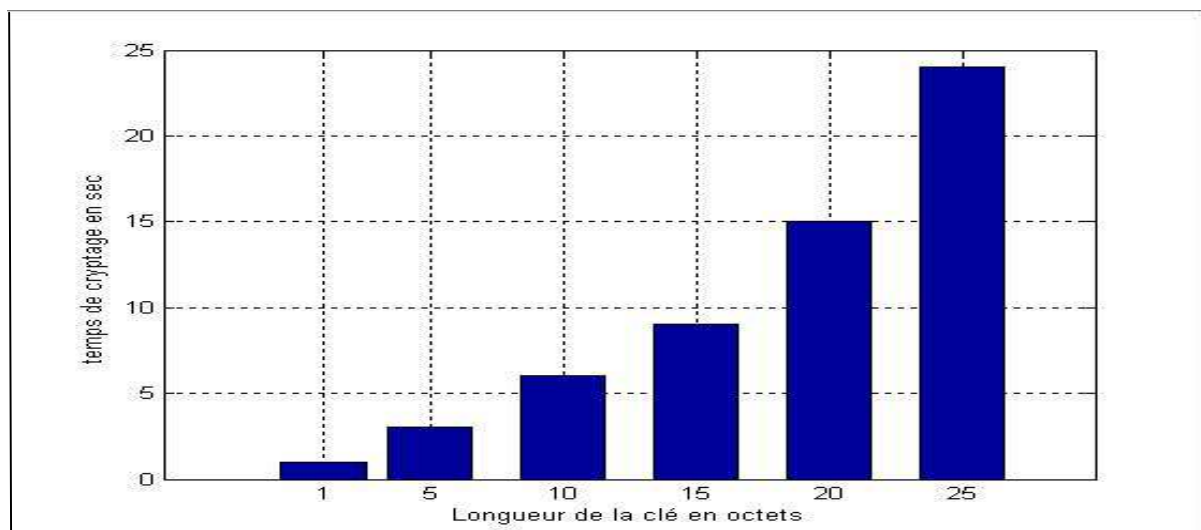


Fig 8: Ciphering time vs. Key length

We notice that the computing time of ciphering/deciphering increase considerably with the two factors (block size and key length). A compromise is necessary to optimize the parameter

and the ciphering quality. The simulation results give an optimum for L=8 to 12 pixels as length of blocks and N=1024 bits for the key.

```

Ciphering key (n,e) : (n :1024 bit) n =
446452067316941072648023979495603096557935206802120707608820935742556402590653163435
526056266409366111947040967524943166790046382329620725379260995602853751441355843530
682269561360921329883650920698017962373169797137894105440958448676685619577366188074
267757958962049105614546746496383184636280719241773335359

e = 28669950953321621413

the ciphered message is C : c= m^e mod n = c =
312888165900803819884980872719331714177149677239888190844807466293971176240682896870
061873408389147567891171770444571752714174072832397200926892936552166085489017014576
580500696646815971210038949992334092934912717266612907413612618968324896612608390001
662190670308737014981055407416186122862216973273248719804208762778573182165468026045
953864810733876346641755687461590757943139110685800768885484641408202083664165979219
809392322678363790034872501672204716122923621918257710562751909410679776409175759329
464304115587520873164739052026160566158794902892023919022972378229999097298536201484
7053610199817915771928152503

Deciphering key (n,d) : d
=
402672364112396539484733354245446480159987502354358797489599926288179288074672286133
110705134828814950663887512715973978155957887007519215890755090147706043865466017003
815388589732637102232433613774621871706061789953517473340199795749080769352304074702
50960438294181749753209502606288198697724669739031398797

Deciphered message is : out= c^d mod n = out =
!(*)+*&" ---- #&(,14<:99862-0++146?JUKA>BC=8552.+ -27@CB@=>DJKHC?=:7487643210,-
/13455654554201343126:IHC?BFE@ @=-;>CFC@54334

out =double(out) = bloc décrypté

033040039041041043042038034032031028029030030031031030029030032035038040044049052060
058057057056054050045048043043049052054063074085075065062066067061056053053050046043
045050055064067066064061062068074075072067063061058055052056055054052051050049048044
045047049051052053053054053052053053052050048049051052051049050054058073072067063066
070069064064061059062067070067064053052051051052

bloc image original : I

033040039041041043042038034032031028029030030031031030029030032035038040044049052060
058057057056054050045048043043049052054063074085075065062066067061056053053050046043
045050055064067066064061062068074075072067063061058055052056055054052051050049048044
045047049051052053053054053052053053052050048049051052051049050054058073072067063066
070069064064061059062067070067064053052051051052
    
```

Fig 9: Example of an implementation of the RSA algorithm

4. Conclusion

In this paper, we implemented an algorithm of encoding and ciphering of a digital image based on the R.S.A algorithm and intended for medical applications. This interface was implanted under Matlab. It is based on a pre-processing of the original image based on a JPEG compression followed by a selective encoding and a vectored quantification. The obtained results demonstrate the importance of an optimization of two parameters:

The segmented block length and the key length. Thus, we studied the effects of variation of these parameters on the deciphered image quality as well as on the processing time and the flow transmission.

REFERENCES

- [1] J.C.Borie, W.Puech, M.Dumas, “ Encrypted Medical Images for Secure Transfer”. International Conference on Diagnostic Imaging and Analysis ICDIA 2002, Shanghai, August 2002, pages 250-255.
- [2] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21, n° 2, pp. 120-126, 1978.
- [3] C.C. Chang, M.S. Hwang, et T-S Chen. “A new encryption algorithm for image cryptosystems”. The Journal of Systems and Software, 58 :83–91, 2001.
- [4] Obo Li, Jason Knipe, Howaed Cheng, “Image compression and encryption using tree structures » Pattern Recognition Letters (1997) , pg 1253-1259.
- [5] S.S.Maniccam, N.G.Bourbakis, “Lossless image compression and encryption using SCAN” . Pattern Recognition 34 (2001) pages 1229-1245.
- [6] B. Schneier, Applied cryptography, Wiley and sons publisher, 1995.
- [7] Borie J.C., Puech W., Dumas M “Crypto-compression system for Secure Transfer of Medical Images”. MEDSIP'04: 2nd Medical Image and Signal Processing, (2004)].
- [8] Abdelmoula Moez, Elloumi Mourad Kamoun Lotfi. "Nouveau schéma de crypto-compression des images médicales " .Revue Informatique, science de l'information et bibliothéconomie, RIST Vol. 13 No 2-2003.