Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 3, March 2021, pp. 1751~1758
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i3.pp1751-1758

Key exchange based on Diffie-Hellman protocol and image registration

Rachid Rimani[1], Naima Hadj Said[2], Adda Ali-Pacha[3], Ozen Ozer[4]
[1,2,3]University of Sciences and Technology of Oran Mohamed Boudiaf, Algeria
[1]University Mustapha Stambouli of Mascara, Algeria
[4]Kırklareli University, Kirklareli, Turkey

Article Info

Article history:

Received May 26, 2020
Revised Oct 30, 2020
Accepted Nov 18, 2020

Keywords:

Concealing the key
Diffie-Hellman
Image registration
Key exchange protocol
Transformed images

ABSTRACT

Nowadays, with the advences in ICT and rapid development of mobile internet; media information shared on the various communication networks requires the existence of adequate security measures. Cryptography becoming an effective way to meet these requirements and for maintain the confidentiality. However, communicating with encrypted messages requires secret key exchange, which is a part of a complex protocol. In this paper, we propose a new method for exchanging key based on Diffie-Hellman protocol and image registration with fast fourier transform, the principle of this method consists to concealing the key in a set of transformed images. Therefore, image registration allows finding transformations between images, which become a tool for recovering the key by the receiver.

Corresponding Author:

Rachid Rimani
Department of Electronics, College of Electrical Engineering
University of Sciences and Technology of Oran Mohamed Boudiaf, Ustomb
P.O. Box 1505 El M'naouar Oran 31000, Algeria
Email: rachid.rimani@univ-usto.dz

1. INTRODUCTION

The In the civilization of information, security issues are essential especially with the globalization of exchanges like internet, messaging, e-commerce. The use of cryptography is indispensable for keeping the confidentiality of information during exchange in the presence of adversaries. However, for a safe use of cryptography we must use a reliable encryption algorithm and secure the exchange of encryption key. Keeping encryption keys safe and secure is not easy. It is usually a question of establishing a secure communication channel. For this, two types of key exchange protocols are used: first the Protocols that assume the prior sharing of information (public key) between the two entities like for example RSA used by HTTPS [1-3]; the second are protocols that assume no prior knowledge of information between the two entities, like the protocol of Diffie-Hellman, which has the advantage of providing retroactive security using the resistance of the discrete logarithm problem and its variants [4]. Today the Diffie-Hellman protocol is widely used on the internet through the TLS protocol; for this invention, Diffie and Hellman received the prestigious Turing Prize in 2016. Protocols of exchanging key have been the subject of numerous studies. For instance, Mohammad Eftekhari [5], propose a protocol for exchanging key with Diffie-Hellman by using a group of matrices over non commutative rings. In [6], Om Pal et all. proposed an ID Based Cryptography for securing a Group of Diffie-Hellman Key Exchange. However, to establish the common key for a group, the scheme uses the identity of the nodes. In [7], Xavier Porte et al. use the phenomenon of identical chaos

synchronization for exchanging key of cryptosystem. In [8], authors proposed a Bi-Symmetric Key Exchange, which improves upon BB84 and Diffie-HellmanMerkle by using some of their key features along with its own and eliminate the need of any dedicated hardware setup for generation of keys and their transmission. In [9], authors developed a quantum key distribution protocol. While to transmit information, the system uses polarized photons. In [10], researchers proposed an efficient scheme of exchanging key and authentication which characterized by a block cipher symmetric using a function of one-way hash, but without using certificates for dual authentication and key exchange.

We propose in this sudie a new method for conceal and transfer the key using Diffie-Hellman protocol and image registration by FFT (fast fourier transform). The key is transmitted using a set of translation applied to images, then send them to the recipient ; such that each translation represents two bytes of the secret key (information to send). Therefore, the performed translations are depended on the size of secret key to be transferred. Images to be transformed are windows selected from the shared original image or their positions varies with each transmission. Recovering key by the receiver is done by registration between received images and the source image.

2. IMAGE REGISTRATION

Image registration consists in establishing a geometric relation between objects represented by two images [11]; this technique is based on the calculation of a spatial transformation function between images in order to superimpose them to the optimum of their resemblance criteria. In [12], image registration is defined as a mapping between two images at a time in space. These images are arrays of two-dimensional of given size denoted *I* and *J*. *I (x, y)* and *J (x, y)* correspond to the intensity values. The mapping between this images is defined by the following expression :

$$J(x,y) = g(I(f(x,y))) \quad (1)$$

f : the transformation of *2D* spatial coordinate ; *g* : the transformation of a *1D* intensity.
I : the reference image and used as a model ; *J* : the target image that will undergo the deformation.

Mathematically, registrate a reference image *S* on the target image *T* defined on a domain $D \in R^2$ or R^3 and with values in R consists in determining the optimal transformation $\widehat{\varphi_\theta} \in E$ (associated space with the transformation) such that $S^{\Psi} := \Psi(S)$ is similar to *T*. [12]

$$\Psi = \text{argmax}_\theta C(S^{\Psi\theta}, T) \quad (2)$$

Ψ is the vector of parameters θ depending on the transformation chosen and its associated space *E*.

An interpolation phase will be necessary to apply the transformation obtained to the target image. argmaxθ indicates the presence of an optimization algorithm of the criterion C, whose evolution gives information on the similarity between the guiding images and the registration system (depending on the choice of criterion, the chosen algorithm may be a minimization). The algorithm stops either when an extreme is reached or at realization of a stop criterion ε (number of iterations, the search step) as shown in Figure 1.

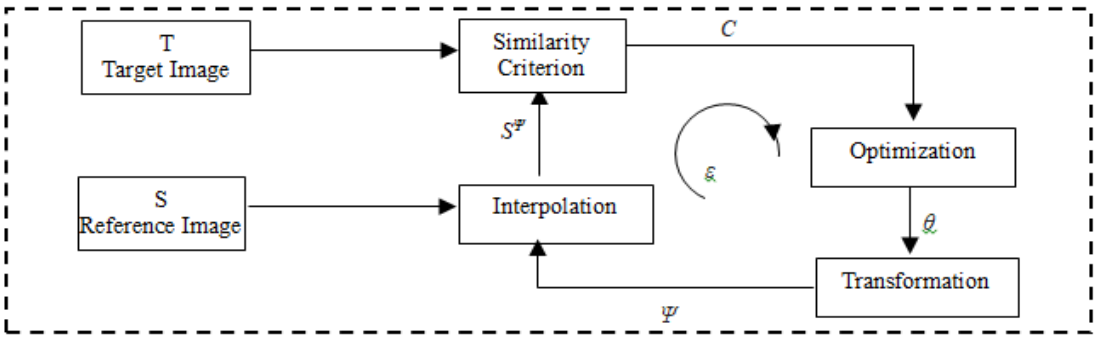

Figure 1. Overall diagram of a registration system

It is sometimes preferred to this definition, a formulation in terms of displacement fields:

$$\Psi = I + U \quad (3)$$

With U the displacement field and I the identity function for any point $X \in D$
We search U such that: $S^U(X) = S(X + U(X))$ is similar to $T(x)$

In fact, whatever the chosen formulation, a registration system consists of four main elements determined according to the application.

a) Primitives: image information guiding the registration system (points, surfaces, gray levels....). We can find the extrinsic methods, which rely on the use of artificial objects and the intrinsic methods, which rely solely on the content of the image; this category can be subdivided into three others: based on internal landmarks [13, 14], based on a pre-segmented structure [15] and based on the pixels properties [16].
b) Transformations can be separated on the basis of several characteristics: according to the field of application (global or local), and according to the categories of elasticity (rigid, affine, projective or curved). [17-20]
c) The criterion of similarity between the images to be registrate (function of the primitives nature);
d) The optimization scheme.

3. IMAGE REGISTRATION BY FFT

The diversity of possible fields of application and the variety of deformations make the registration a very open problem in the field of the research and therefore studied under different points of view. To extract translation and rotation parameters of a geometric transformation of similarity type between two images, we will focus on iconic registration approach global using the phase correlation technique [21-23], the Fourier spectral representation and the Log-Polar representation [24].

Images are a priori complex and considered as functions of $\mathbb{R}2$ in $\mathbb{C}$; for this reason we will model the problem of image registration by DFT (Discrete Fourier Transform) with 2 dimensions characterised by the followed mathematical expression.

$$DFT(I)(p,q) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} I(m,n)e^{-j2\pi pm/M}e^{-j2\pi qn/N} \quad (4)$$

I is a discrete image of size MxN

To make the process of image registration faster, we replace the DFT by FFT (Fast Fourier Transform) which gives faste results in execution time and robust to noise. The technique of registration with FFT is based on rotation property and translation property deduced from the delay theorem.

3.1. Translation property (correlation phase)

We denoted *g0* and *g1* the two functions with two variables, that represent the gray levels of two images which differ by a displacement *(u, v)*:

$$g1(x, y) = g0(x-u, y-v) \quad (5)$$

Such as *(x, y)* denoted a point in the signal space and *(fx, fy)* denoted a point of the frequencie space. The FFT is given by (6) :

$$G1(fx, fy) = F[g0(x-u, y-v)] \quad (6)$$

$$= e^{-2i\pi(u\,fx + v\,fy)} G0(fx, fy)$$

We can deduced that $|G1(f_x, f_y)| = |G0(f_x, f_y)|$; so the amplitude spectra are invariant by translation. Therefore, the information on the translation parameters is contained in the phases of these two transforms. To extract them, we apply the technique of correlation phase and calculate the IFT (Inverse Fourier Transform) of the result as shown in Figure 2.

$$\psi(fx,fy) = G1(fx,fy)/G0(fx,fy) = e^{-2i\pi(u\,fx + v\,fy)} \quad (7)$$

Such $\psi(f_x, f_y)$ is the cross-power spectrum (ratio of the spectra) between *go* and *g1*.

ψ gives a wave monochromatic; the calculation of Inverse Fourier Transform of ψ, we find the Dirac function which is non-zero at the point *(u,v)* as shown in Figure 3.

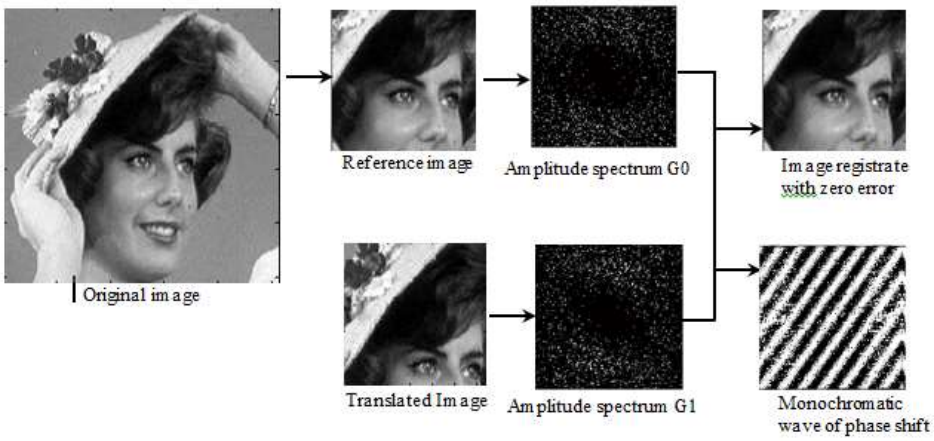

Figure 2. Registration between using translation property

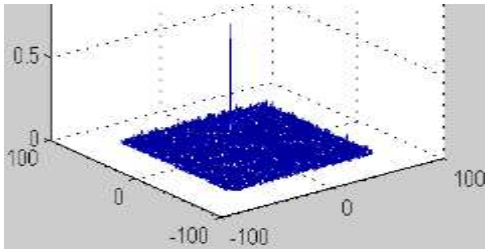

Figure 3. Dirac function corresponding to the translation

3.2. Rotation property

Let's *g0* and *g1* the two functions differ by an angle of rotation *α.*

$$g1(x,y)=g0(x\cos(\alpha)-y\sin(\alpha),\ x\sin(\alpha)+y\cos(\alpha)) \quad (8)$$

The Fourier transforms of functions *g0* and *g1* is given by the following expressions:

$$G1(f_x,f_y)=F[g0(x\cos(\alpha)-y\sin(\alpha),\ x\sin(\alpha)+y\cos(\alpha))]$$

$$= G0(f_x\cos(\alpha)-f_y\sin(\alpha),\ f_x\sin(\alpha)+f_y\cos(\alpha)) \quad (9)$$

We notice from (9) that the amplitude spectra of two images differ by an angle of rotation *α.* So, extracting the parameter of rotation between the two images is like extracting their Fourier spectra, given the better readability of the rotation between the images of spectra than between the original images Figure 4.

By taking the expression (8) linking two images in rotation by an angle α and by passing from the cartesian system to the log-polar transform (LPT) which makes it possible to pass from parameters of rotation into simple parameters of translation ; to extract them we exploit the phase correlation technique with a change of variables; so the expression (8) becomes :

$$g1(\rho,\theta) = g0(\rho,\theta-\alpha) \quad (10)$$

With $\rho = log(\sqrt{x^2+y^2})$ and $\theta = \arctan(\frac{y}{x})$ are the new considered variables. Therefore,

So, we can note that the rotation of an angle α becomes a parameter of translation this along the angular axis in the polar coordinate system. The pixel values of transformed images in LPT are not necessarily integer. Therefore, they are not necessarily coincide on a pixel in the new presentation of the image; so we must use a resampling technique (bilinear interpolation) to solve this problem.

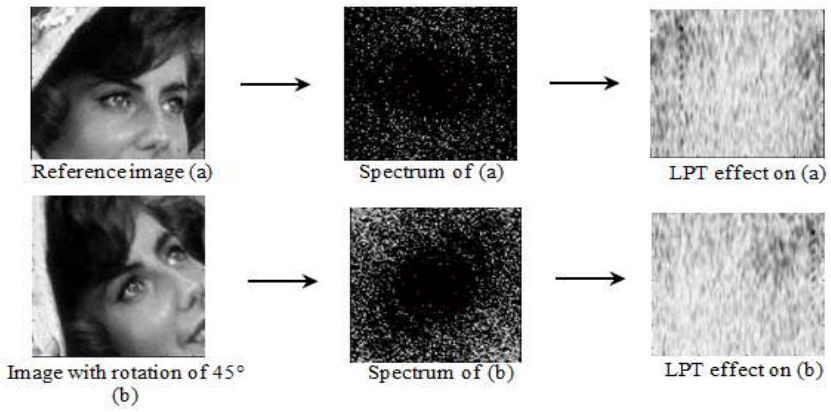

Figure 4. Registration using rotation property

4. KEY EXCHANGE WITH DIFFIE-HELLMAN PROTOCOL

The key exchange security with Diffie-Hellman protocol is based on the difficulty of calculating discrete logarithms [25, 26], a difficult problem as in the case of El Gamal. The key value depends on the participants (and information about their private and public keys).

To exchange a secret key *K* of size *t* bytes. The interlocutors ***A*** and ***B*** have a finite cyclic group *G* and a generator *a* of this group (the elements of *G* are therefore, if we multiplically note the operation of the group: *1, a, a 2, · · ·, a s−1* where *K* is the order of *G*). Take for example *G* the multiplicative group $(Z / pZ)^*$, where *p* is a large prime number and *a* an element generating this group (but it could also be a generator of a large subgroup of $(Z / pZ)^*$).

The Figure 5 shows the key exchange procedure. The calculations indicated are made in group *G*, therefore in our example modulo p.

- Public data: the group $G = (Z / pZ)*$, generator *a* from this group, mask generator *h*.
- ***A*** draws an integer *n* such that $1 < n < p - 1$ and keeps it secret.
- ***A*** sends a^n to ***B*** (calculation done in the group, so here modulo *p*).
- ***B*** draws an integer *m* such that $1 < m < p - 1$ and keeps it secret.
- ***B*** sends a^m to ***A***.
- ***A*** calculates $K_{AB}=\mathbf{Y_B}^n \pmod p = (\mathbf{a^m})^n \bmod p$
- ***B*** calculates $K_{BA}=\mathbf{Y_A}^m \pmod p = (\mathbf{a^n})^m \bmod p$
- ***A*** and ***B*** share now the same key $K_{AB}= K_{BA}$

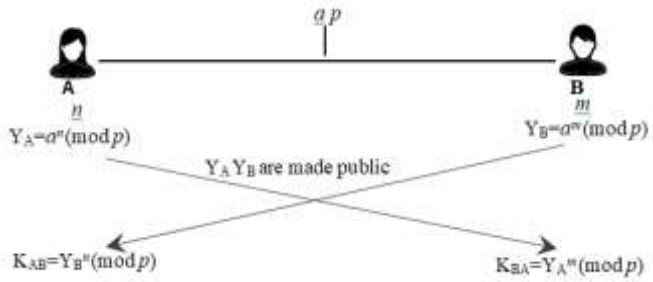

Figure 5. Diffie-Hellman principle

5. CONTRIBUTION: KEY EXCHANGE BASED ON DIFFIE-HELLMAN PROTOCOL AND IMAGE REGISTRATION

5.1. Overview

The detection of rotation and translation peaks gives the good results of image registration. However, experimental results allows determining that when transformed image is not combined by translation and rotation, the registration error is zero; otherwise, the error is greater than 0 because of the resampling step; for

this reason we use just translation for Exchanging key with the proposed method. Therefore, the key Exchang by image registration consists to hide and transfer the key in set of transformed images using a secret image already shared between transmitter and receiver. so, the secret key to be sent is divided into blocks of the same size of 2 bytes (each transformation T_x, T_y represents 2 bytes), then a set of translated images is generated according to each block and sent to the receiver. The recipient must registrate the received images on the source image to find the T_xT_y transformations, then form the data blocks (secret key) as illustrated in Figure 6.

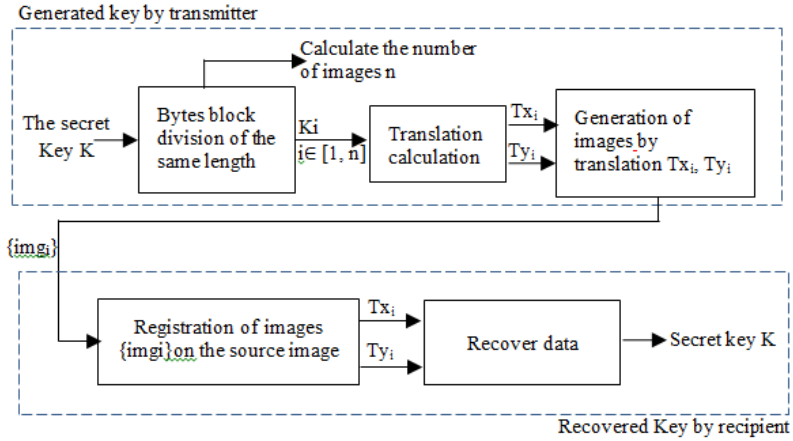

Figure 6. Global scheme of key exchange by image registration

5.2. Full example of exchanging Key by Diffie-Hellman protocol and image registration

The following example as shown in Figure 7 shows how the transmitter and the recipient share 2 bytes using the proposed method of exchanging Key with Diffie-Hellman protocol and image registration and by exploiting the delay theorem of FFT. First, the transmitter A and the recipient B share the same translated image (10,30), this image is registrated with the second translated image (13,22) by transmitter. The registration result (-3, 8) is sent to the recipient.

The receiver will follow the same procedure, so shared image (10,30) will registrated with the translated image (6,42) by recipient. The results of registration (4,-12) is sent to transmitter

The shared secret : registration between translated image (13,22) by transmitter A and received image (4,-12) by B gives the same results with registration between translated image (6,42) by recipient B and received image (-3,8) by A

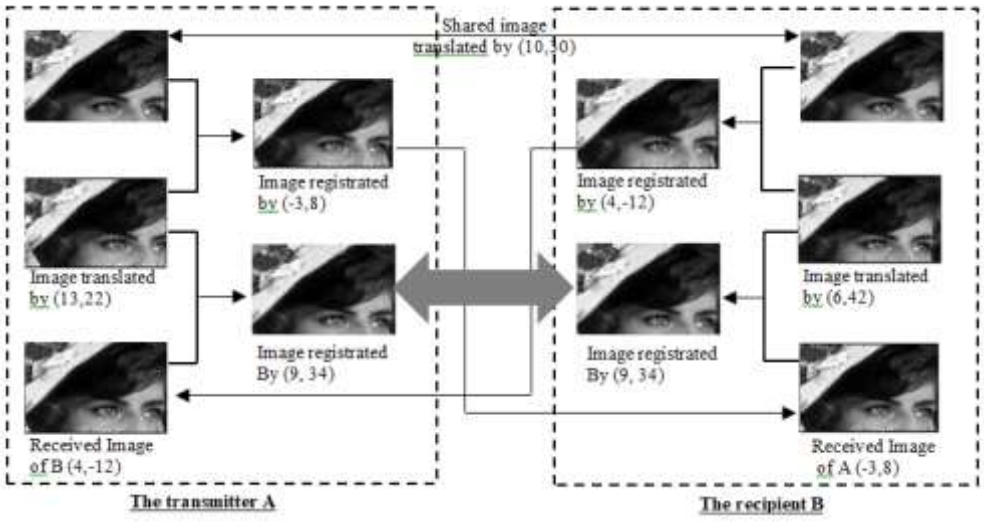

Figure 7. Example of key exchange by Diffie-Hellman protocol and image registration

5.3. Improvement

In order to avoid the estimation of information and increase the security level of the proposed protocol; we have synchronized the sending of translated images by a permutation of pseudo random numbers without repetition generated by chaos (according to number of images to be send).

st = 4 6 1 7 2 5 3 is the obtained permutation using a logistic map of parameters μ=3,9 and X0=0,1. So transformed images TxiTyi will be sent in the order of the permutation st : Tx4Ty4 Tx6Ty6 Tx1Ty1 Tx7Ty7 Tx2Ty2 Tx5Ty5 Tx3Ty3. The recipient must generate the same sequence of pseudo-random numbers using the same parameters to have the synchronization of received images in Figure 8.

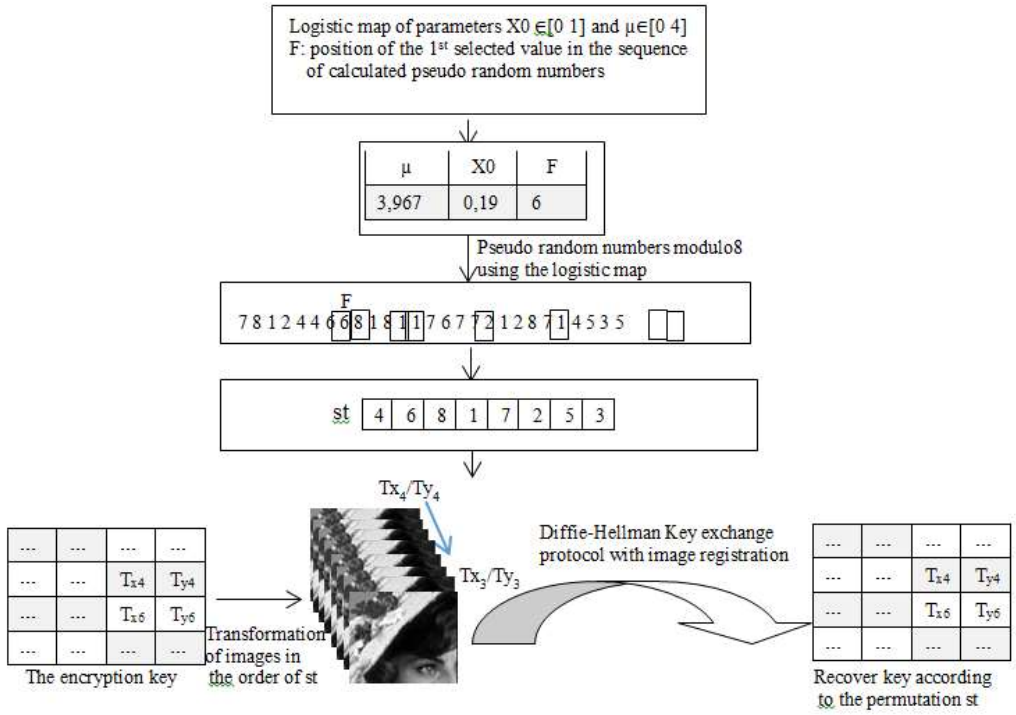

Figure 8. Diagram of synchronization and exchanging an encryption key

6. CONCLUSION

We introduced in this study a new key exchange method based on Diffie-Hellman protocol and image registration, which consists dissimulating the transfer of the secret key in a set of transformed images. These images are registrating by using the correlation phase of FFT to find the required transformations. To get a good results of image registration we must used an appropriate images (very rich in information) and if the secret key have an important size we can used a video instead of transformed images sequence. In the proposed key exchange method by Diffie-Hellman protocol and image registration, we used just the translation to send two bytrs of data, but if the transformation of the image is combined by translation, rotation and a homothetic that reduce the number of transferred images.

REFERENCES

[1] R. Cramer, V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," *Advances in Cryptology — Lecture Notes in Computer Science, Springer*, vol 1462, pp.13-25, 1998. DOI: https://doi.org/10.1007/ bfb0055717

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method of obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[3] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *in IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985. DOI: 10.1109/TIT.1985.1057074.

[4] H. Corrigan-Gibbs, D. Kogan, "The Discrete-Logarithm Problem with Preprocessing," *Advances in Cryptology – Lecture Notes in Computer Science. Springer*, vol 10821, pp 415-447, 2018. DOI: https://doi.org/10.1007/978-3-319-78375-8_14

[5] Mohammad Eftekhari, "A Diffie-Hellman key exchange using matrices over non commutative rings," *Groups, complexity and cryptology*, vol. 4, no. 1, pp. 167-176, 2012.
[6] Om Pal, Anupam Saxena, Uttam Kumawat, Ravi Batra, Zia Saquib, "Secure Group Diffie-Hellman Key Exchange with ID Based Cryptography, *" Second International Conference on Advances in Communication, Network, and Computing, CNC 2011*, 2011.
[7] Xavier Porte, M.C. Soriano, Daniel Brunner, Ingo Fischer, "Bidirectional private key exchange using delay-coupled semiconductor lasers, " *Optics Letters, Optical Society of America*, vol. 41, no. 12, pp. 2871-2874, 2016.
[8] S. Sonthalia, T. Mandal, Chakraborty M, "Bi-symmetric Key Exchange: A Novel Cryptographic Key Exchanging Algorithm, " *International Ethical Hacking Conference*. *Advances in Intelligent Systems and Computing. Springer*, vol. 811, pp. 91-102, 2019. DOI:https://doi.org/10.1007/978-981-13-1544-2_8
[9] C.H. Bennett, G. Brassard, "Quantum cryptography: public key distribution and coin tossing, " *Theoretical Computer Science*, vol. 560, no. 1, pp. 7-11, 2014. DOI:https://doi.org/10.1016/j.tcs.2014.05.025
[10] L. Yonghwan, C. Eunmi, and M. Dugki, "An Authenticated Key Exchange Mechanism Using One-Time Shared Key," *Computational Science and Its Applications – ICCSA*, vol. 4, no. 2, pp. 187-194, 2005.
[11] M. Wyawahare, P. Patil, H. Abhyankar, "Image Registration Techniques: An overview, " *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 2, no. 3, pp. 11-26, 2009.
[12] Kessler, M, "Image registration and data fusion in radiation therapy," *British Journal of Radiology*, vol. 79, no. 1, pp. 99-108, 2006.
[13] Pietrzyk U. Herholz K., Fink G., Jacobs A., Mielke R., Slansky I., Wtirker M., Heis W. "An interactive technique for three dimensional image registration: validation for PET,SPECT, MRI and CT brain studies," *Journal of nuclear medicine*, vol. 35, no. 12, pp. 2011-2018, 1994.
[14] J.P Thirion. "Extremal Points: deffinition and application to 3D image registration," *Computer Vision and Pattern Recognition, IEEE Computer Society Press*. pp. 587-592, 1994.
[15] C.A Pelizzari, G.T.Y Chen, D.R Spelbring, R.R Weichselbaum & C.T. Chen. "Accurate three-dimensional registration of CT, PET, and/or MR images of brain," *Journal of Computer Assisted Tomography*, vol. 13, pp. 20-26, 1989.
[16] O. Migneco, "Applications du recalage d'images de médecine nucléaire", *Service de Médecine Nucléaire - Centre A. Lacassagne- Nice, Revue de TACOMEN*, vol. 5, no. 2, 1999.
[17] J.B.A. Maintz, M.A. Viergever, "A survey of medical image registration," *Medical Image Analysis*, vol. 2, no. 1, pp. 1-36, 1998.
[18] Makela, T., Clarysse, P., Sipila, O., Pauna, N., Pham, Q. C., Katila, T., Magnin. "A review of cardiac image registration methods," *IEEE Transactions on MedicalImaging*. vol. 21, no. 9, pp. 1011-1021, 2002.
[19] Van den Elsen, P., Pol, E., Viergever, M. "Medical image matching-a review with classification," *IEEE Engineering in Medicine and Biology Magazine.* vol. 12, no. 1, pp. 26-29, 1993.
[20] Veltkamp, R., Hagedoorn, M. State of the art in shape matching. Principles of Visual Information Retrieval, pp. 87-119, 2001.
[21] S.Ghorbel, A.Khalfallah, M.S.Bouhlel. "Study and Evaluation of Correlation Techniques and Phase Correlation Techniques: Application for Image Registration". *5th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications SETIT* March 22-26, 2009 – TUNISIA, 2009.
[22] Y. Keller, A. Averbuch, O. Miller. "Robust phase correlation". *17th International Conference on Pattern Recognition*, vol. 2, pp. 740-743, 2004.
[23] B.Marcel, M.Briot, R. Murrieta. "Calculation of translation and rotation by the Fourier transformation," *Signal processing*, vol. 14, no. 2, pp. 135-149, 1997.
[24] J. Sarvaiya, S. Patnaik, S. Bombaywala. "Image registration using log-polar transform and phase correlation," *TENCON 2009-IEEE 10th Region Conference*, pp. 1-5, 2009.
[25] V. I. Nechaev, "Complexity of a determinate algorithm for the discrete logarithm," *Mathematical Notes*, vol. 55, no. 2, pp.165-172, 1994. DOI: https://doi.org/10.1007/bf02113297
[26] V. Shoup, "Lower bounds for discrete logarithms and related problems," *Advances in Cryptology - Lecture Notes in Computer Science- Springer*, vol. 1233, pp. 256-266, 1997. DOI: https://doi.org/10.1007/3-540-69053-0_18