Volume 2, No. 4, April 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at http://www.jgrcs.info

Transmission of Large Information through KAP Using Non-Abelian Group

Abhishek Dwivedi[2*], Deo Brat Ojha[1], Ajay Sharma[2], Ramveer Singh[2] and Awakash Mishra[2]

[1]Professor, Department of Mathematics,Raj Kumar Goel Institute of Technology,
[2]Research Scholar Singhania University, Jhunjhunu, Rajsthan, India
5th K.M. Stone Delhi – Meerut Road,Ghaziabad, U.P.201003,INDIA
E-mail: dwivediabhi@gmail.com,ojhdb@yahoo.co.in

ABSTRACT: *Anyone can send a confidential message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient. It is really appreciable method to provide high security to the medical image or patient's information. Which provide us integrated secure transmission of medical information like Image, Audio, Video etc. with a common key. We also use lossless compression technique like SEQUITUR for efficient utilization of communication channel. The combination of encryption with compression provides confidentiality in the transmission.*

Keywords: *Key agreement protocol, Cryptography, Braid group, steganography SEQUITUR algorithm.*

INTRODUCTION

The necessity of fast and secure diagnosis is vital in the medical world to save the life of world creature. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the net [12,13,14]. For image transmission, two different approaches of technologies have been developed. The first approach is based on content protection through encryption [21]. In this approach, proper decryption of data requires a key. The second approach bases the protection on digital watermarking or data hiding, aimed at secretly embedding a message into the data. In the current era, the transmission of Image over internet is so much challenging over the internet. In this manner, the better way to transmit the image over internet is encryption. Using the cryptography we secure the image as well as also better utilization of the communication channel with compression technique.

Cryptography is a tool of security that aims to provide security in the ciphers of any kind of messages.

Cryptographic algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption.

A common cryptographic technique generally, encrypted each individual conversation or data with a separate key. This is called a session key, because it is used for only one particular communication session,[1]. Ko et al [4] proposed a braid group version of Diffie-Hellman key agreement, Man- in- the- middle attack works on this protocol. Since the path breaking work of Diffie -Hellman in 1976, several key agreement protocols have been proposed over the years [5,6,7,8,9,10,11].

In this current article, we describe SEQUITUR, an algorithm that infers a hierarchical structure from a sequence of discrete symbols. The ability to deal easily with long sequences has greatly extended the range of SEQUITUR's application. This arrangement distributes in different phases and each phase plays an important role in manner.

PRELIMINARIES:

2.1 Braid Groups:

Emil Artin [3] in 1925 defined B_n, the braid group of index n, using following generators and relations: Consider the generators $\sigma_1, \sigma_2, \ldots\ldots\sigma_n$, where σ_i represents the braid in which the $(i+1)^{st}$ string crosses over the ith string while all other strings remain uncrossed. The defining relations are

1. $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $|i-j| \geq 2$,

2. $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ for $|i-j| = 1$

An n-braid has the following geometric interpretation: It is a set of disjoint n-strands all of which are attached to two horizontal bars at the top and at the bottom such that each strands always heads downward as one walks along the strand from the top to the bottom. In this geometric interpretation, each generator σ_i represents the process of swapping the i^{th} strand with the next one (with i^{th} strand going under the $(i+1)^{th}$ one). Two braids are equivalent if one can be deformed to the other continuously in the set of braids. B_n is the set of all equivalence classes of geometric n-braids with a natural group structure. The multiplication *ab* of two braids *a* and *b* is the braid obtained by positioning *a* on the top of *b*. The identity *e* is the braid consisting of *n* straight vertical strands and the inverse of *a* is the reflection of a with respect to a horizontal line.So σ^{-1} can be obtained from σ by switching the over-strand and under-strand.

$\Delta = (\sigma_1, \sigma_2 \ldots\ldots\ldots \sigma_{n-1})(\sigma_1, \sigma_2 \ldots\ldots\ldots \sigma_{n-2}) \ldots\ldots\ldots\ldots (\sigma_1, \sigma_2)(\sigma_1)$

is called the fundamental braid.

We describe some mathematically hard problems in braid groups. We say that x and y are conjugate if there is an element a such that $y = axa^{-1}$. For $m < n; B_m$ can be considered as a subgroup of B_n generated by σ_1, σ_2 ……… σ_{m-1}.

DIFFIE-HELLMAN KEY AGREEMENT (DHKA)

Suppose that A and B want to agree on a shared secret key using the Diffie-Hellman key agreement protocol [2]. They proceed as follows: First, A generates a random private value a and B generates a random private value b. Then they derive their public values using parameters p and g and their private values. A's public value is ga mod p and B's public value is gb mod p. They then exchange their public values. Finally, A computes kab = (gb)a mod p, and B computes kba = (ga)b mod p. Since kab = kba = k, A and B now have a shared secret key k.

Braid Group Version of DHKA Using Conjugacy Problem

Ko et al. [5] proposed a braid group version of Diffie-Hellman key agreement protocol. Let B_n be a braid group where CSP is infeasible. As mentioned earlier, all the braids in Bn are assumed to be in the left canonical form. Thus for a, b in B_n, it is hard to guess a or b from ab.

Initial set up:

A sufficiently complicated n-braid $x \in B_n$ for a large n is selected and is known to both the parties A and B.

Key agreement:

(a) A chooses a random secret braid $a \epsilon LB_n$ computes axa^{-1} and sends it to B.

(b) B chooses $a \in UB_n$ computes bxb^{-1} and sends to A.

(c) A receives bxb^{-1} and computes $a(bxb^{-1})a^{-1}$.

(d) B receives axa^{-1} and computes $b(axa^{-1})b^{-1}$.

Compression

A compression scheme can be employed what is known as lossless compression on secrete message to increase the amount of hiding secrete data, a scheme that allows the software to exactly reconstruct the original message [15].

The transmission of numerical images often needs an important number of bits. This number is again more consequent when it concerns medical images. If we want to transmit these images by network, reducing the image size is important. The goal of the compression is to decrease this initial weight. This reduction strongly depends of the used compression method, as well as of the intrinsic nature of the image. Therefore the problem is the following:

1. To compress without lossy, but with low factor compression. If you want to transmit only one image, it is satisfactory. But in the medical area these are often sequences that the doctor waits to emit a diagnostic.

2. To compress with losses with the risk to lose information. The question that puts then is what the relevant information is to preserve and those that can be neglected without altering the quality of the diagnosis or the analysis. The human visual system is one of the means of appreciation, although subjective and being able to vary from an individual to another. However, this system is still important to judge the possible causes of degradation and the quality of the compression [16].

THE SEQUITUR ALGORITHM

The SEQUITUR [17] algorithm represents a finite sequence as a context free grammar whose language is the singleton set {σ}. It reads symbols one-by-one from the input sequence and restructures the rules of the grammar to maintain the following invariants:

(A) no pair of adjacent symbols appear more than once in the grammar, and

(B) Every rule (except the rule defining the start symbol) is used more than once. To intuitively understand the algorithm, we briefly describe how it works on a sequence 123123. As usual, we use capital letters to denote non-terminal symbols. After reading the first four symbols of the sequence 123123, the grammar consists of the single production rule S ➔ 1, 2, 3, 1 where S is the start symbol. On reading the fifth symbol, it becomes S ➔ 1, 2, 3, 1, 2 Since the adjacent symbols 1, 2 appear twice in this rule (violating the first invariant), SEQUITUR introduces a non-terminal A to get

S ➔ A, 3,A A ➔1, 2

Note that here the rule defining non-terminal A is used twice. Finally, on reading the last symbol of the sequence 123123 the above grammar becomes

S ➔ A, 3, A, 3 A ➔ 1, 2

This grammar needs to be restructured since the symbols A, 3 appear twice. SEQUITUR introduces another non-terminal to solve the problem. We get the rules

S ➔ B,B B ➔ A 3 A➔ 1 2

However, now the rule defining non-terminal A is used only once. So, this rule is eliminated to produce the final result.

S ➔ B, B B ➔ 1, 2, 3

Note that the above grammar accepts only the sequence 123123.

OUR APPROACH:

In our proposed scheme, we use sequitur as a compression technique and Key Agreement technique for a common key, which give us improved result. Sequitur is a single-pass hierarchical algorithm that builds a context-free grammar for a string. The resulting grammar compactly represents the original structure and has the interesting property that the compressed format itself contains useful information about the string.

Input a medical image and follows these phases:

Phase 1: Generating $n \times n$ blocks

In RGB space the image is split up into red, blue and green images. The image is then divided into 8×8 blocks of pixels and accordingly the image of $w \times h$ pixels will contain $W \times H$ blocks. Where, $W = w/8$, $H = h/8$.

Phase 2: DCT

All values are level shifted by subtracting 128 from each value. The Forward Discrete Cosine Transform of the block is then computed. The mathematical formula for calculating the DCT is:

$$T(u,v)=\sum_{x=0}^{n}\sum_{y=0}^{n} f(x,y),g(x,y,u,v)$$

Where ,

$$g(x,y,u,v)=\frac{1}{4}\alpha(u)\alpha(v)\cos\left[\frac{(2x+1)u\pi}{2n}\right]\cos\left[\frac{(2y+1)v\pi}{2n}\right]$$

Where $\alpha(u)=\begin{cases}\frac{1}{\sqrt{2}}\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots\ldots\ldots\ldots..\text{for. } u=0\\ 1\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\text{for. } u=1,2,\ldots.N-1\end{cases}$

Phase 3: Quantization

Quantization is the step where the most of the compression takes place. DCT really does not compress the image, as it is almost lossless. Quantization makes use of the fact that, the high frequency components are less important than the low frequency components. The Quantization output is

INITIAL SET UP

P_b : Sufficiently complicated n-Braid

$p \in LB_n$ Known as Alice private key.

Id_A = Alice's Identity.

$q \in UB_n$ Known as Bob private key, and

Id_B = Bob's Identity.

$X_A = pP_b p^{-1}$ Known as Alice public

$$Q_{DCT}=\text{round}(\frac{T(u,v)}{Z(u,v)})$$

The $Z(u,v)$matrix could be anything, but the JPEG committee suggests some matrices which work well with image compression.

Phase 4: Compression using SEQUITUR

After quantization, the scheme uses a filter to pass only the string of non-zero coefficients. By the end of this process we will have a list of non-zero tokens for each block preceded by their count.

DCT based image compression using blocks of size 8x8 is considered. After this, the quantization of DCT coefficients of image blocks is carried out. The SEQUITER compression is then applied to the quantized DCT coefficients.

Phase 5:

In this section [21] we describe our two-pass biased key agreement protocol to agree on a common key to encrypt the medical image or other information about the patient. Our protocol works in the following steps.

Key Agreement

Alice		**Bob**
Choose $x \in LB_n$ And $r' \in LB_n$ Calculate $X = x \square Id_A$ And $R = r' \square Id_A$ And $C_A = p(X) \oplus X_B(R)$ …………(1) And also Calculate $M_A = xP_b x^{-1}$ Alice decrypt $X_A(R')$ with its private key p. Then i.g. $C_B \Theta X_A(R') = q(Y)$ ------(3) and Alice encrypt $q(Y)$ with its public key $X_B(q(Y))$ and find Y and Alice verify that Y contain Id_B as suffix, Alice know the identity of bob.	$\xrightarrow{C_A}$ $\xleftarrow{C_B}$	Choose $y \in UB_n$ And $r'' \in UB_n$ And $Y = y \square Id_B$ And $R' = r'' \square Id_B$ And $C_B = q(Y) \oplus X_A(R')$ ………(2) Bob decrypt $X_B(R)$ with its private key q. Then i.g $C_A \Theta X_B(R) = p(X)$ ------(4) and bob encrypt $p(X)$ with its public key $X_A(p(X))$ and find X and bob verify that X contain Id_A as suffix, bob know the identity of Alice.
Firstly, to find out the identity of each other, both make some calculation as		
Calculate $k_A (= k_B) = pX_B p^{-1}$ And $Key_A = xk_A^{-1} M_B k_A x^{-1}$	$\xrightarrow{M_A}$ $\xleftarrow{M_B}$	Calculate $k_B = qX_A q^{-1}$ And $M_B = k_B y M_A y^{-1} k_B^{-1}$ Calculate $key_B = yM_A y^{-1}$
• In each above step, if Key_A or key_B is I ,then the protocol run is terminated with failure. • So both Alice and Bob have secret key $K = Key_A = key_B$ and both can communicate secretly for that session.		

All above phases shown in diagrammatic in figure 1

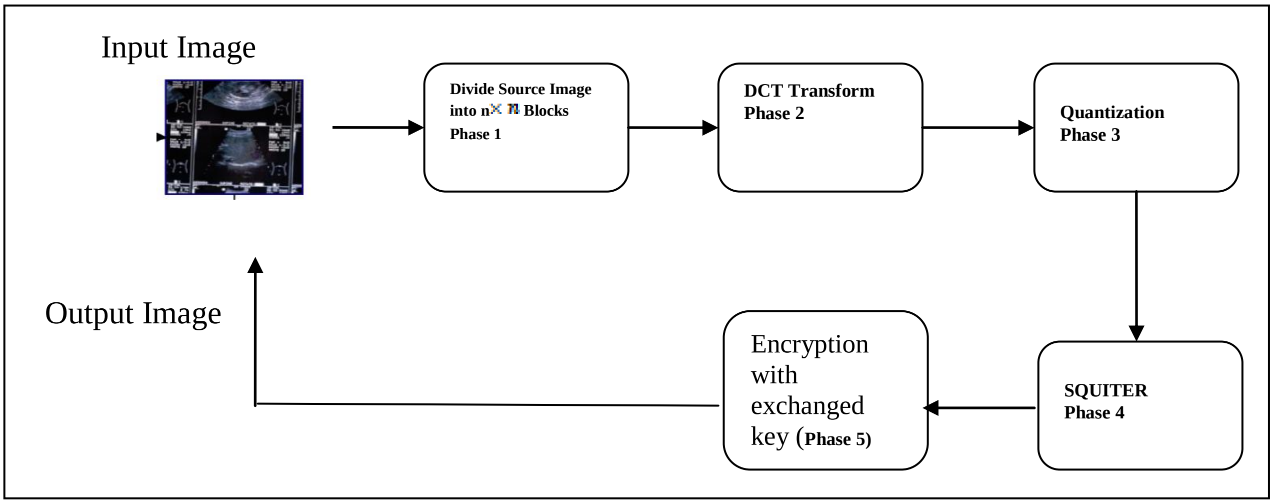
Input Image
Divide Source Image into n× n Blocks Phase 1
DCT Transform Phase 2
Quantization Phase 3
SQUITER Phase 4
Encryption with exchanged key (Phase 5)
Output Image

Figure 1: Diagrammatic Approach

So at the receiving end, reverse the process in all phases, we can get the required medical information.

CONCLUSION:

Freeness to send confidential information like Image, Audio, Video etc. using public information, but the sensitive information can only be decrypted with a private key kept by the intended recipient.

In the new scenario the Health Insurance Portability and Accountability Act (HIPAA) [19] requires that medical providers and insurance companies implement procedures and policies to protect patient's medical information.

In this paper, here we use sequitur as a compression technique and key agreement protocol to agree on a common key, Sequitur has the ability to read a stream in reverse also. So our approach is more appropriate, secure and futuristic than previous literature of medical data transmission.

REFERENCE:

[1] Bruce Schneier "applied cryptography, second edition" John wiley &sons, Inc.

[2] W. Diffie and M.Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.

[3] E. Artin, "Theory of braids," Annals of Mathematics, vol. 48, pp. 101-126, 1947.

[4] K. Ko, S. Lee, J. Cheon, J. Han, J. kang C. Park. New public key cryptosystem using braid groups, Crypto'2000, LNCS 1880, pp.166-183, Springer 2000.

[5] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Van-stone, "An Efficient Protocol for Authenticated Key Agreement", Technical Report CORR98-05, Department of CO, University of Waterloo, 1998.

[6] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Van-stone, "An efficient protocol for authenticated key agreement," Design, Codes and Cryptography, vol.28, no. 2, pp. 119-134, 2003.

[7] A. Menezes, M. Qu, and S. Vanstone, "Key agree-ment and the need for authentication," in Proceedings of PKS'95, pp. 34-42, 1995.

[8] S. B. Wilson, D.Johnson, and A. Menezes,"Key agreement protocol and their security analysis," in Proceedings of Sixth IMA International Conference on Cryptography and Coding, pp. 30-45, 1997.

[9] Atul Chaturvedi, Sunderlal" An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups", in International Journal of Network Security Vol.6 No.2 p.p. 181-184, March, 2008.

[10] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, Relations among notions of security for public-key encryption schemes, Advances in Cryptology | CRYPTO '98, Lecture Notes in Computer Science, 1462 (1998), Springer-Verlag, pp. 26-45.

[11] R.Dutta, R. Barua and P. Sarkar,"Pairing Based Cryptography : A Survey Cryptology e-print Archive ", Report 2004/064,2004.

[12] G. Lo-varco,W. Puech, and M. Dumas. "Dct-based watermarking method using error correction codes", In ICAPR'03, International Conference on Advances inPattern Recognition, Calcutta, India, pages 347–350, 2003.

[13] R. Norcen, M. Podesser, A. Pommer, H.P. Schmidt, and A. Uhl. "Confidential storage and transmission of medical image data", Computers in Biology and Medicine, 33:277–292, 2003.

[14] Diego F. de Carvalho, Rafael Chies, Andre P. Freire, Luciana A. F. Martimiano and Rudinei Goularte, "Video Steganography for Confidential Documents: Integrity, Privacy and Version Control" , University of Sao Paulo – ICMC, Sao Carlos, SP, Brazil, State University of Maringa, Computing Department, Maringa, PR, Brazil.

[15] Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" Applied Computer Science Department, Faculty of Information Technology, Philadelphia University, Jordan

[16] Borie J., Puech W., and Dumas M., "Crypto-Compression System for Secure Transfer of Medical Images", 2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004), September 2004.

[17] N.Walkinshaw, S.Afshan, P.McMinn "Using Compression Algorithms to Support the Comprehension of Program Traces" Proceedings of the International Workshop on Dynamic Analysis (WODA 2010) Trento, Italy, July 2010.

[18] Johannes Buchmann, Carlos Coronado, Martin D¨oring, Daniela Engelbert, Christoph Ludwig, Raphael Overbeck, Arthur Schmidt ,Ulrich Vollmer, Ralf-Philipp Weinmann, "Post- Quantum Signatures",eprint.iacr.org/2004/297.

[19] "Health Insurance Portability and Accountability Act (HIPAA) and Its Impact on IT Security," Regulatory Compliance Series 3 of 6, Apani Networks White Paper Compliance Series. May 12, 2005. http://www.apani.com.

[20] V.Pless, " Introduction to theory of Error Correcting Codes", Wiley , New York 1982.

[21] D.B.Ojha, Abhishek Dwivedi, Ajay Sharma, Ramveer Singh, "Non-repudiable biased bitstring key Agreement Protocol with non Abelian-group", International Journal of engineering Science and technology. Vol. 2(9), 2010, 4162-4166