A New Image Encryption Approach using Combinational Permutation Techniques

A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna

Abstract— This paper proposes a new approach for image encryption using a combination of different permutation techniques. The main idea behind the present work is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. This paper presents an approach for a random combination of the aforementioned permutations for image encryption. From the results, it is observed that the permutation of bits is effective in significantly reducing the correlation thereby decreasing the perceptual information, whereas the permutation of pixels and blocks are good at producing higher level security compared to bit permutation. A random combination method employing all the three techniques thus is observed to be useful for tactical security applications, where protection is needed only against a casual observer.

Keywords— Encryption, Permutation, Good key, Combinational permutation, Pseudo random index generator.

I. Introduction

COMMUNICATION security is an application layer technology to guard any transmitted information (starting from speech, image to computer messages) against unwanted disclosure as well as to protect the data from unauthorized modification while in transit. There are three basic methods of secured communication available, namely, cryptography, steganography and watermarking. Among these three, the first one, cryptography [1]-[3], deals with the development of techniques for converting information between intelligible and unintelligible forms during information exchange. Steganography [4]-[5], on the other hand, is a technique for hiding and extracting information to be conveyed using a carrier signal. The third one, watermarking [6]-[8], is a means of developing proper techniques for hiding proprietary information in the perceptual data.

In secured communications using cryptography, which is the main focus of the present work, the information under consideration is converted from the comprehensible form to incomprehensible structure using certain coding operations at the transmitter. The unintelligible or encrypted form of the information is then transmitted through the insecure channel to the destination. Such an encryption technique provides privacy of a message with respect to any unauthorized recipient since it is in ungraspable shape for such an user. At the intended recipient side, however, the information is again converted back to understandable form using decryption operation (essentially an inverse operation of encryption) and thus the message is conveyed securely. It should be noted that both these encryption and decryption operations are guided by specific keys, where the keys may be same or one can be easily derived from the knowledge of the other. Such cryptographic techniques are grouped under private key cryptography [3], [9]. Alternately, encryption and decryption keys may be different or computationally it may not be feasible to derive one key even though the knowledge of other key is available, and such cryptographic methods are known as public key cryptography [2]. Further, the security needed may be against two types of attackers, namely, casual listeners/observers or professional unauthorized recipients, termed as cryptanalysts. In the former case, the security is needed only in terms of hours while in the later it may be in terms of years. The duration roughly indicates the amount of time that is needed to analyze the information available in unintelligible form in the insecure channel without the knowledge of keys to derive the underlying information. The scenario where security is needed against casual listener/observer, the cryptographic structure should be as simple as possible in order to reduce the cost. The present work focuses on development of improved private key cryptographic methods for providing security against such casual observers in the context of image communications.

In designing private key cryptographic techniques, permutation methods [10]-[11] and pseudo random sequence generators [12]-[13] play important roles for their simple yet effective information coding performances. The proposed method uses many good keys (discussed later), selected using pseudo random index generators, for different permutation operations. Since a large number of keys are used, the security level offered is also high. Further, the amount of redundant information available in the encrypted image is kept as low as possible, thereby providing fairly high security level against casual observers. The security is usually achieved with the knowledge of information to be exchanged. In particular, in our case (i.e., image communication), the image is represented as a group of bits, pixels and blocks and therefore, the encryption is done by permuting the respective groups. Further, to make it more robust against casual attacks, a random combinational image encryption approach with bit, pixel and block permutations is proposed. It is also shown in results that

Manuscript received February 28, 2006.

A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna are with the Department of Electronics and Communication Engineering, Indian Institute of Technology Guwahati, North Guwahati - 781039, India. E-mail: a.mitra@iitg.ernet.in, subba@iitg.ernet.in and prasanna@iitg.ernet.in.

if the random combinational sequence of permutations is not known to the observer, it will not be possible for him/her to retrieve the original information, even if the permutation private keys are known to that person.

The paper is organized as follows. In Section II, we deal with the permutation techniques for image encryption where, in particular, we discuss about pseudo random index generators, fundamentals of permutations and the three basic permutation methods for encrypting images in different subsections. The proposed scheme with combinational permutation techniques is introduced in Section III. Section IV presents the results and also briefs about the effectiveness of the proposed scheme. The paper is concluded by summarizing the present work along with the scope of future work in Section V.

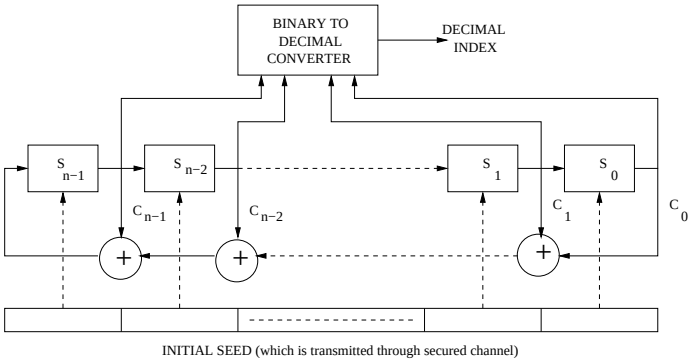


Fig. 1. Structure of a general pseudo random index generator.

II. Permutation Techniques for Image Encryption

As indicated earlier, in designing private key cryptographic techniques, permutation methods are considered as important building blocks in conjunction with pseudo random sequence generators for selecting a specific permutation key from a given list of good keys. Here, we first discuss about the pseudo random generators, followed by fundamentals of permutation techniques and a brief description of three different permutation methods in the context of image communications.

A. Pseudo Random Index Generator

Pseudo random index generator (PRIG) for permutation purpose is usually constructed using the linear feedback shift registers (LFSR) [12]-[13]. A PRIG contains n shift registers and is initiated with a starting seed, which is usually transmitted through a secured channel for intended users only. The outputs of the shift registers are multiplied with the coefficients $(C_{n-1}, C_{n-2}, \ldots, C_1, C_0)$ of a primitive polynomial with respect to mod-2 operation. The resultant output obtained by the modulo operation is then fed back to the first shift register. The shift register output values are converted into decimal index using binary to decimal converter. The general structure of such a PRIG is shown in Fig. 1. Note that the periodicity of such a random index generator is 2^{n-1}.

B. Fundamentals of Permutation

A permutation process of degree n refers to the operation of replacing an arrangement $\{p_i | i = 1, 2, \cdots, n, p_i \in S\}$ by a second arrangement $\{q_i | i = 1, 2, \cdots, n, q_i \in S\}$, and is represented as

$$\phi = \begin{pmatrix} p_1 p_2 \cdots p_n \\ q_1 q_2 \cdots q_n \end{pmatrix} \quad (1)$$

where $n!$ such permutations are possible and S denotes any non-empty set. The reverse of this permutation process is specified as

$$\phi^{-1} = \begin{pmatrix} q_1 q_2 \cdots q_n \\ p_1 p_2 \cdots p_n \end{pmatrix} \quad (2)$$

which retrieves the original arrangement. The above method is formally defined as follows.

Definition 1: Permutation is a one-to-one mapping of any non-empty set S onto S. The set containing all such mappings is denoted by S_n with $n!$ members, if S has n elements. Note that every group under consideration is isomorphic[1] to a group of permutations.

Based upon this definition, the cryptography process, with the help of permutation operation, can be defined as follows.

Definition 2: If any data matrix X is transformed to a cipher-matrix $\psi_z = \phi_z(X)$ where ϕ_z is any permutation operation, then the original matrix X can be obtained again from ψ_z with the inverse operation of ϕ_z on it, i.e., $\phi_z^{-1}(\psi_z) = \phi_z^{-1}(\phi_z(X)) = X$, as $\phi_z^{-1}\phi_z$ forms an identity operator.

It is known that every permutation is a product of transpositions. If a permutation is a product of even number of transpositions, it is called even permutation. In S_n, $\frac{n}{2}!$ permutations are even and rest $\frac{n}{2}!$ are odd. However, in most of these permutations, all the elements may not be displaced from its position. Certain residual intelligence thus would be present even after the permutation process, which can be useful for attackers. Therefore instead of taking all the permutations in account, certain specific permutation patterns that increase the security level are considered only and are called good permutation keys. Good permutation keys are useful for reducing the intelligible information having the properties: (a) displacement of each element from its own location, (b) adjacent elements' appearance in different order, and, (c) high average shift factor [14]. Average shift factor (ASF) implies average shift of the all elements in a given permutation key. Clearly, the maximum value of ASF is obtained from the inverse identity permutation, which, at all, is not desirable from security view point. The other keys with high ASF and minimum residual intelligence can then be considered as good keys. It is presented in the form of the following definition.

Definition 3: A good permutation key, after obeying property (a) and (b) above, yields an ASF $\frac{1}{n}\sum_{i=1}^{n} D(e_i) \geq \frac{n}{3}$

[1]Let G and H be two groups and λ an operator. Then a homomorphism λ: G $\rightarrow$ H is said to be an isomorphism of G into H if λ is one-to-one.

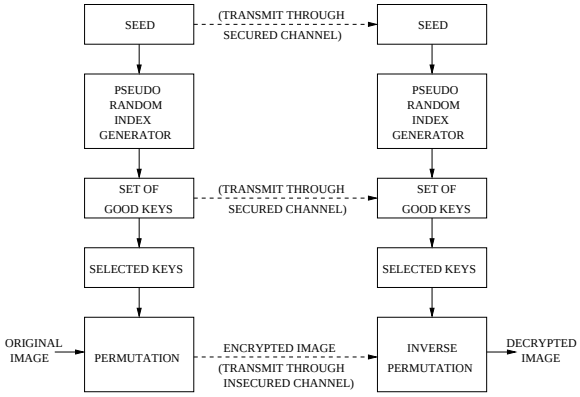


Fig. 2. The general block diagram of permutation schemes.

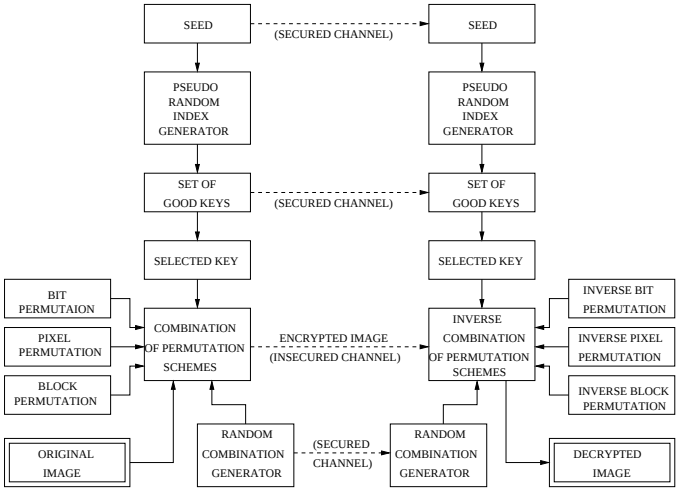


Fig. 3. The block diagram of proposed combinational permutation schemes.

$\forall n \in \mathbf{Z}_p$, where $D(e_i)$ means the net displacement of the ith element.

In the proposed method, the set of good keys are stored in a table and a random one is selected from this set by pseudo random index generator.

C. The Basic Permutations for Encrypting Images

In the context of images, there exist three basic permutation techniques, as discussed below.

1) Bit permutation: The image can be seen as an array of pixels, each with eight bits for 256 gray levels. In the bit permutation technique the bits in each pixel taken from the image are permuted with the key chosen from the set of keys by using the pseudo random index generator. The entire array of these permuted pixels forms the encrypted image. The encrypted image obtained from the bit permutation technique is transmitted to the receiver through the insecure channel. At the receiver the encrypted image is decrypted using the same set of keys and same pseudo random index generator. As the number of bits in each pixel is eight, we also take the key length equal to eight. The number of permutations obtained with eight elements is 8! (=40320) but the number of good keys formed by such eight elements is 121 only [14]. Therefore, to get 127 keys using a PRIG of maximal length 127, other 6 keys are taken randomly from these 121 good permutation keys to form the complete set.

2) Pixel permutation: In this scheme each group of pixels is taken from the image. The pixels in the group are permuted using the key selected from the set of keys. The encryption and decryption procedure is same as the bit permutation technique. The size of the pixel group is same as the length of the keys, and all the keys are of same length. If the length of the keys is more than the size of pixel group, the perceptual information reduces. In this work the group of pixels is taken along the row without the loss of generality, i.e., the column wise procedure would yield same kind of results.

3) Block permutation: In this technique the image can be decomposed into blocks. A group of blocks is taken from the image and these blocks are permuted same as bit and pixel permutations. For better encryption the block size should be lower. If the blocks are very small then the objects and its edges don't appear clearly. In this block permutation the blocks are permuted horizontally in the image. The permutation of blocks along vertical side is also similar to horizontal side block permutation. At the receiver the original image can be obtained by the inverse permutation of the blocks.

A general block diagram of the permutation methods is shown in Fig. 2, where the block *permutation* represents any of the above three discussed procedures.

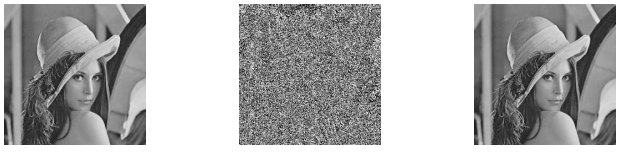
III. The Proposed Scheme with Combinational Permutation Techniques

Here we present a new approach for image encryption using a combination of different aforesaid permutation techniques. The main idea behind the present work is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain random permutation techniques. This is achieved by deploying the following technique. From minute observation, Definition 2 as presented in Section II can be extended to the following Corollary.

Corollary 1: Any data matrix, transformed to a cipher matrix ψ' with n different permutations $\phi_1, \phi_2, \ldots, \phi_n$ sequentially i.e., $\psi' = \phi_n(\phi_{n-1}(\ldots(\phi_1(X))\ldots)$ can be restored again with inverse operation of ϕ_i $(i = 1, 2, \ldots, n)$ in inverse sequence, i.e., $X = \phi_1^{-1}(\phi_2^{-1}(\ldots(\phi_n^{-1}(\psi'))\ldots)$.

Proof: It directly follows Definition 2 with operator order extension. ■

Such a Corollary, when applied in tandem with random permutation generators, can provide better security in terms



(a) (b) (c)

Fig. 4. Results of bit permutation. (a) Original image. (b) Encrypted image. (c) Decrypted image.

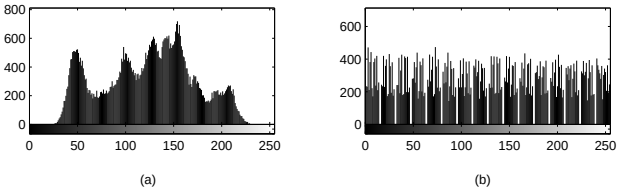


Fig. 5. Histograms of bit permutation. (a) Original image. (b) Encrypted image.

(a) (b) (c)

Fig. 6. Results of pixel permutation. (a) Original image. (b) Encrypted image. (c) Decrypted image.

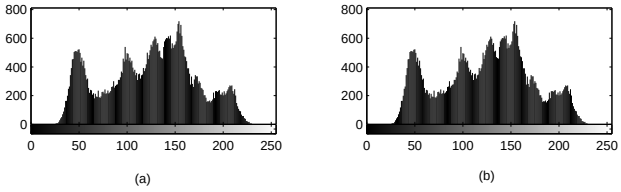


Fig. 7. Histograms of pixel permutation. (a) Original image. (b) Encrypted image.

of any kind of attack, provided ϕ_i $(i = 1, 2, \cdots, n)$ are chosen randomly from any standard set of operations. The same is proposed in the scheme with a random combination of bit, pixel and block permutations. The advantage offered by such a scheme is that even if the private key is known to the attacker somehow and the random combination key is unknown, then the person will not be able to extract/tamper the image. Also, as the combination of these three approaches the redundancy, visual intelligence reduces. To get back the original image at the receiver, the order of the permutation processes should be exactly reverse to the order at the transmitter, otherwise the output will produce no visible information. Therefore, this random combination seed is also sent to destination via secured communication channel. The block diagram of the proposed method is shown in Fig. 3.

IV. Results and Discussions

The proposed combinational scheme along with individual permutations has been implemented in the *Matlab* with several test images. Below are some results applied on the standard *Lena* gray scale image.

A. Basic permutations

Fig. 4 shows the results of *bit permutation* technique. Here, the encrypted image appears as a random noisy image as the lower significant bits move towards the most significant bits and vice versa. Generally the most significant bits represent more details about the image. The lower significant bits are appeared as noise. So the encrypted image has less visual intelligence. Bit permutation is better approach in image encryption according to perception. The histograms of original & encrypted images are shown in Fig. 5. In the histogram of the encrypted image the nearly uniform random distribution of gray levels is achieved. Fig. 6 shows the results of *pixel permutation* technique. In the pixel permutation eight pixels are taken as a group and permuted with the same size key. The same set of keys for bit permutation is used here. However, the image obtained is nearly similar to the original image due to high correlation between the adjacent pixels. But the edges are slightly distorted in the encrypted image. The histograms of original & encrypted images are shown in Fig. 7. The histogram of the encrypted image is same as the histogram of the original image. In this method the pixel values are same after encryption but their position will be changed, leading to same histograms. Fig. 8 shows the results of *block permutation* technique. The encrypted image here has more visual intelligence. Here, if the block size is small then it is difficult to decrypt. Using the edges of the objects it is easy to find the original image from the encrypted image. In these results blocks are of size 8×8. Here the same 8 element key set is stored in a table. The blocks are permuted along the horizontal side. In this technique, the histogram of encrypted image is almost similar to that of Fig. 7 and therefore is not shown here.

B. Proposed combinational technique

In this method the order of the bit, pixel and block permutations is random. Here we have shown the results with the combination of [block, bit, pixel] permutation respectively. The encrypted noisy image due to this combination is shown in Fig. 9. Generally after the bit permutation the encrypted image will be appeared as a noisy image. But the pixel and block permutation methods make much stronger from the security point of view. The decrypted image can be obtained as original image by having a reverse permutation of [pixel, bit, block] combination only, otherwise the received image is garbled. The histogram of the encrypted image with this combinational technique is shown in Fig. 10 and Fig. 11 shows

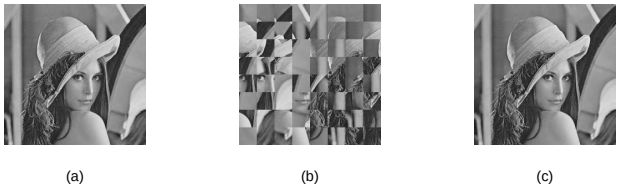


Fig. 8. Results of block permutation. (a) Original image. (b) Encrypted image. (c) Decrypted image.

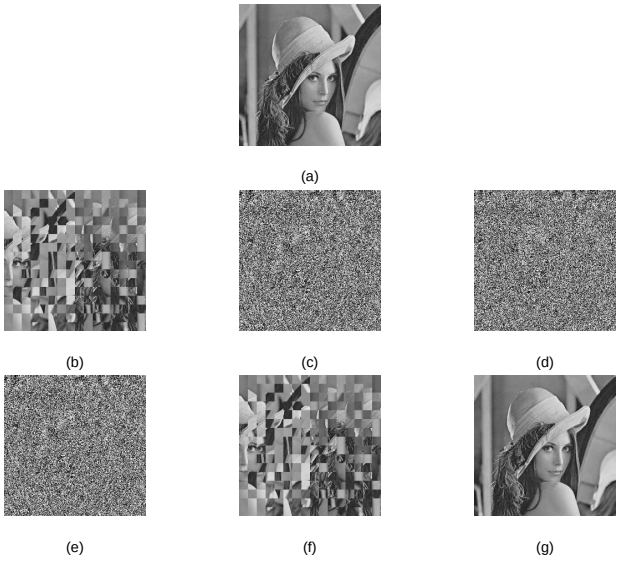


Fig. 9. Results of the proposed technique with [block, bit, pixel] combination. (a) Original image. (b), (c), (d) Encrypted images with the above sequential combination in order. (e), (f), (g) Decrypted images using inverse permutations with [pixel, bit, block] combination sequentially.

the effectiveness of the proposed method by taking another random combination [block, bit, pixel] at the receiving end, where the received image is totally noisy.

V. Conclusions

A simple-to-implement yet effective method has been proposed in this paper for image encryption using a combination of different permutation techniques. The main idea stems from the fact that the perceivable information in an image can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. This paper has presented an approach for a random combination of the aforementioned permutations for image encryption. From the results, it is observed that combined method achieves the advantages all individual permutation techniques and overcomes the limitations of these methods, e.g., visual intelligence and redundancy. A further extension of the approach is possible by using variable length keys with the information available to the receiver via PRIG indices, thereby increasing the level of security significantly.

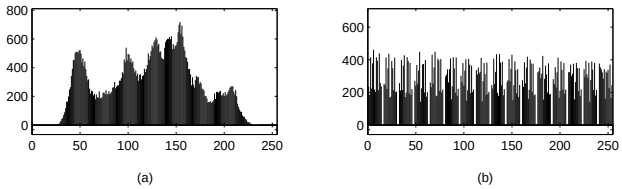


Fig. 10. Histograms of images. (a) Original image. (b) Final encrypted image with the combination mentioned in Fig. 9.

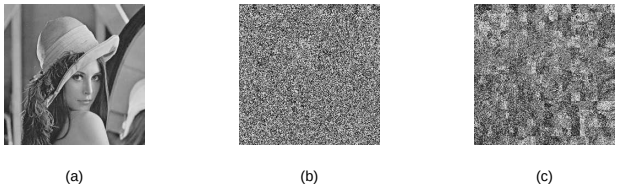


Fig. 11. Effectiveness of the proposed method. (a) Original image. (b) Encrypted image with [block, bit, pixel] combination. (e) Decrypted image using inverse permutation with [block, bit, pixel] combination, leading to a garbled information.

References

[1] A. J. Elbirt and C. Paar, "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography," *IEEE Trans. Parallel and distributed systems*, vol. 16, no. 5, pp. 468-480, May 2005.
[2] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, vol. 22, no. 6, pp. 644-654, Nov. 1976.
[3] W. Stallings, *Cryptography and Network Security*. Englewood Cliffs, NJ: Prentice Hall, 2003.
[4] E. Besdok, "Hiding information in multispectral spatial images," *Int. J. Electron. Commun. (AEU)* 59, pp. 15-24, 2005.
[5] S. Trivedi and R. Chandramouli, "Secret Key Estimation in Sequential Steganography," *IEEE Trans. Signal Processing*, vol. 53, no. 2, pp. 746-757, Feb. 2005.
[6] Y. Wu, "On the Security of an SVD-Based Ownership Watermarking," *IEEE Trans. Multimedia*, vol. 7, no. 4, pp. 624-627, Aug. 2005.
[7] Y. T. Wu and F. Y. Shih, "An adjusted-purpose digital watermarking technique," *Pattern Recognition* 37, pp. 2349-2359, 2004.
[8] A. Masoud and A. H. Tewfik, "Geometric Invariance in Image Watermarking," *IEEE Trans. Image Processing*, vol. 13, no. 2, pp. 145-153, Feb. 2004.
[9] S. S. Maniccam and N. G. Bourbakis,"Image and video encryption using scan patterns," *Pattern Recognition* 37, pp. 725-737, 2004.
[10] P. P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications," *IEEE Trans. Consumer Electronics*, vol. 46, no. 3, pp. 395-403, Aug. 2000.
[11] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 118-129, March 2003.
[12] L. T. Wang and E. J. McCluskey, "Linear Feedback Shift Register Design Using Cyclic Codes," *IEEE Trans. Computers*, vol. 37, no. 10, pp. 1302-1306, Oct. 1988.
[13] A. Fuster and L. J. Garcia, "An efficient algorithm to generate binary sequences for cryptographic purposes," *Theoretical Computer Science* 259, pp. 679-688, 2001.
[14] S. R. M. Prasanna *et. al.*, "Study of Permutations in the Context of Speech Privacy," in *Proc. ECCAP 2000*, Chennai, Jan. 2000, pp. 99-106.