World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:2, No:2, 2008

An Image Encryption Method with Magnitude and Phase Manipulation using Carrier Images

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

Abstract— We describe an effective method for image encryption which employs magnitude and phase manipulation using carrier images. Although it involves traditional methods like magnitude and phase encryptions, the novelty of this work lies in deploying the concept of carrier images for encryption purpose. To this end, a carrier image is randomly chosen from a set of stored images. One dimensional (1-D) discrete Fourier transform (DFT) is then carried out on the original image to be encrypted along with the carrier image. Row wise spectral addition and scaling is performed between the magnitude spectra of the original and carrier images by randomly selecting the rows. Similarly, row wise phase addition and scaling is performed between the original and carrier images phase spectra by randomly selecting the rows. The encrypted image obtained by these two operations is further subjected to one more level of magnitude and phase manipulation using another randomly chosen carrier image by 1-D DFT along the columns. The resulting encrypted image is found to be fully distorted, resulting in increasing the robustness of the proposed work. Further, applying the reverse process at the receiver, the decrypted image is found to be distortionless.

Keywords— Encryption, Carrier images, Magnitude manipulation, Phase manipulation.

I. Introduction

SECURING communications is an important aspect in the present era of digital and wireless communication. The objective of communication security is to protect the message from unauthorized users. There are three major ways of securing communications, namely, cryptography, steganography and watermarking. Cryptography [1]-[6] basically deals with developing methods for converting messages from intelligible form to unintelligible form. Steganography [7]-[10] is a means of proposing methods for hiding messages inside other messages. Watermarking, [11]-[14] on the other hand, is a technique for hiding authentication information inside messages. All the methods mentioned above, however, are on the condition to retrieve the message from unintelligible or hidden form when it is needed. In the present work, our focus has been on the first method, cryptography.

In cryptography, message is transformed from intelligible to unintelligible form using the *encryption* operation and is converted back from unintelligible to intelligible form using the *decryption* operation [1], [15]-[17]. Note that the main component of either encryption or decryption, which is essentially an inverse operation of encryption, is termed as *key*, where the security of a given encryption method is directly proportional to the length of the key. If the same key is used for both encryption and decryption, then it is called a private-key cryptosystem [3], [18]. Alternatively, if the encryption and decryption keys are different, then it is called a public-key cryptosystem [1].

The private-key cryptosystem employs either permutation or substitution or both and is dictated by the method employed. Most of these methods operate in temporal or spatial domain. In frequency domain, the cryptosystem employs frequency inversion, band scarmbling and permutation of spectral features like linear prediction coefficients (LPCs) [1], [19]. In all these cases, the encryption is dictated by the key and if some how the key is known, then the unauthorized users can decrypt the message. The objective of this work is to increase the level of security by using carrier images, such that not only the key but also the carrier images are needed to decrypt the message.

The proposed method, dealing with private key cryptosystem, works in the frequency domain. The basis for the proposed method is that the encrypted signal is obtained by magnitude and phase manipulation of the original message using the carrier signal. The original message magnitude and phase can be uniquely retrieved from the encrypted signal if and only if the carrier signal magnitude and phase are known. Since the carrier signal is kept secret along with the keys, mere retrieval of key will not be able to decrypt the message. The complexity is increased further by randomly choosing the carrier signal from the set of signals. In simple sense, what is available in the insecured channel is the combined signal and the message can be obtained from this only if the carrier signal is known.

This paper is organized as follows: in Section II, the general block diagrams of the existing and proposed private-key cryptosystems are discussed. The proposed magnitude manipulation, phase manipulation and the combined magnitude and phase manipulation methods for encryption are introduced with details in Section III. The experimental results and discussions related to the same are given in Section IV. The paper is concluded by providing the summary of the present work and the scope of the future work in Section V.

II. Private-Key Cryptosystem using Carrier Images

The general block diagram of a private-key cryptosystem is given in Fig. 1. As indicated in the figure, a private-key

Manuscript received February 20, 2006.

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

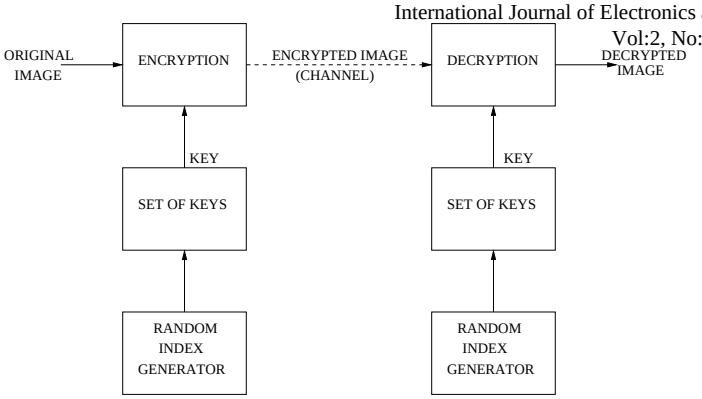

Fig. 1. Block diagram of private-key cryptosystem.

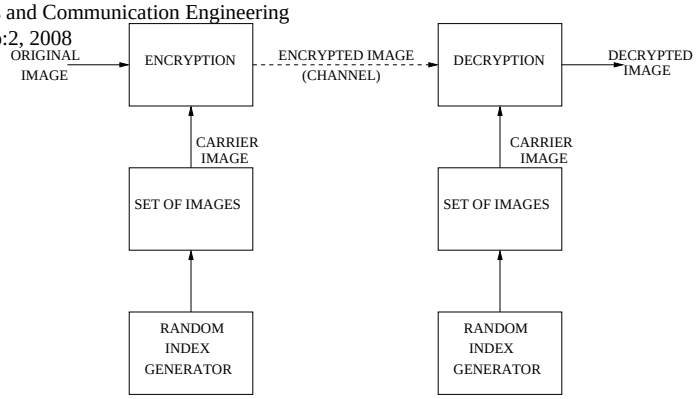

Fig. 2. Block diagram of proposed private-key cryptosystem using carrier images.

cryptosystem consists of an encryption method and a key. The key for encryption is randomly selected from a set of stored keys using a random index generator. The random index generator is essentially a linear shift register configured to generate a pseudo-random decimal integer sequence [1]. The encrypted message (image) is obtained by performing encryption on the original message (image) using the selected key. The encrypted message is transmitted via the insecured channel. At the receiver, the encrypted message is applied to a decryption operation along with the same key chosen for encryption. This is done by maintaining the same set of keys and synchronizing the random index generators at both the transmitter and receiver sides. The output of the decryption operation is the decrypted message which in ideal condition (no distortion) will be the original message (image). This assumption is made in this paper throughout the discussion.

The block diagram of the proposed private-key cryptosystem is shown in Fig. 2. As indicated in the figure, the original image to be encrypted is applied to the encryption method. A carrier image is randomly chosen from the set of images using a random index generator. The row or column encryption operation by either magnitude manipulation or phase manipulation or both (to be discussed next) is performed using the carrier image. The encrypted image is transmitted via the insecured channel. At the receiver side, the encrypted image is applied to the decryption operation and the original image is obtained by performing magnitude manipulation or phase manipulation or both using the same carrier image used for encryption. This is done by maintaining the same set of images and synchronizing the random index generators at both the transmitter and receiver sides. The output of the decryption operation will be the original image.

III. Encryption Methods using Carrier Images

The basis for the proposed methods is that the original image can be retrieved from the encrypted image only when the carrier image is made available. The manipulation of the magnitude and phase of the original image is subjected to the condition of satisfying even symmetry for magnitude manipulation and odd symmetry for phase manipulation. This is to ensure the retrieval of the encrypted or decrypted images in the spatial domain.

A. Encryption by magnitude manipulation

The block diagram of the proposed magnitude manipulation method for encryption and decryption is shown in Fig. 3. One dimensional (1-D) Discrete Fourier Transform (DFT) is computed for the original image to be encrypted along the rows/ columns [20]. Similarly, a carrier image is selected from the set of images using a random index generator and row/ column wise 1-D DFT is computed for the selected carrier image. A row/ column is randomly selected from the 1-D DFT values of the original image using a random index generator. Similarly, a row/ column is randomly chosen from the 1-D DFT values of the carrier image. The magnitude addition is done for the two and scaled by a factor of 0.5. The scaling is done to keep the magnitude of the encrypted image at comparable level to that of the two images. Now, the phase of the selected row/ column of the original image is used for constructing the encrypted version of that row and stored as first row in the encrypted image. Random selection of row/ column of the original and carrier images is made from the remaining ones, magnitude manipulation is performed and the encrypted version is stored as the second row in the encrypted image. This procedure is continued till all the rows/columns in the original image are completed. The encrypted image is constructed in the spatial domain by taking the Inverse Discrete Fourier Transform (IDFT) of the encrypted version in the frequency domain. In other words, if $\mathbf{U}(m,n)$ and $\mathbf{C}(m,n)$ denote the input and carrier images, their 1-D DFTs, $\mathbf{U}'(m,l)$ and $\mathbf{C}'(m,l)$ respectively, are calculated using the following equations:

$$\mathbf{U}'(m,l) = \sum_{n=0}^{N-1} \mathbf{U}(m,n)\mathbf{W}_N^{ln}, \qquad 0 \le m,l \le N-1 \quad (1)$$

$$\mathbf{C}'(m,l) = \sum_{n=0}^{N-1} \mathbf{C}(m,n)\mathbf{W}_N^{ln}, \qquad 0 \le m,l \le N-1 \quad (2)$$

where $\mathbf{W}_N^{ln} = e^{-\frac{j2\pi ln}{N}}$. Let $\lambda(.)$ denotes a random operator which selects any row of a matrix at a random within the range $[0, N-1]$ without replacement. Then, any row vector $\mathbf{v}(k,l)$, $k = 0, 1, \cdots N-1$ can be written as

$$|\mathbf{v}(k,l)| = \frac{1}{2}\left[\left|\lambda_1\big(\mathbf{U}'(m,l)\big)\right| + \left|\lambda_2\big(\mathbf{C}'(m,l)\big)\right|\right] \quad (3)$$

where λ_1 and λ_2 denote two independent operators. This vector contains the magnitudes of two randomly added rows of $\mathbf{U}'(m,l)$ and $\mathbf{C}'(m,l)$, which, in turn, would produce a magnitude manipulated matrix $|\mathbf{V}(m,l)| = [|\mathbf{v}(0,l)|\ |\mathbf{v}(1,l)| \cdots |\mathbf{v}(N-1,l)|]^T$ to be used for our case. The encrypted image with frequency domain can then be written as

$$\mathbf{V}(m,l) = |\mathbf{V}(m,l)|e^{j\Phi\left(\mathbf{U}'(m,l)\right)} \quad (4)$$

where $\Phi\big(\mathbf{U}'(m,l)\big)$ represents the phase given by $\mathbf{U}'(m,l)$. The conversion of ***V(m,l)*** from frequency domain into spatial domain is as follows:

$$v(m,n) = \frac{1}{N}\sum_{l=0}^{N-1} \mathbf{V}(m,l)\mathbf{W}_N^{-ln}, \qquad 0 \le m,n \le N-1. \quad (5)$$

In the decryption process, the row/ column DFT is computed for the encrypted image and is scaled by a factor of 2. The row/ column DFT of the carrier image selected during the encryption is computed. Magnitude of the encrypted image is subtracted from the carrier image. The subtraction is dictated by the random index generator selecting the rows/ columns of the carrier image. The magnitude spectrum of the original image is obtained from the magnitude manipulated image using the same independent operators λ_1 and λ_2, i. e. ,

$$\left|\lambda_1\big(\mathbf{U}'(m,l)\big)\right| = 2|\mathbf{v}(k,l)| - \left|\lambda_2\big(\mathbf{C}'(m,l)\big)\right|. \quad (6)$$

The original image in the frequency domain is reconstructed by rearranging the rows and columns using the random index generator. The original image is reconstructed in the spatial domain by using the phase of the encrypted image, which is nothing but the phase of the original image and the subtracted magnitude and then taking IDFT.

B. Encryption by phase manipulation

The block diagram for the encryption by phase manipulation remains essentially same as that for the magnitude manipulation, except for the magnitude manipulation blocks in the encryption and decryption replaced by phase manipulation blocks. Along the similar lines of encryption by magnitude manipulation, in this case, instead of the magnitude of original image, the phase is manipulated using the following equation:

$$\Phi\big(\mathbf{v}(k,l)\big) = \frac{1}{2}\left[\Phi\big(\lambda_3(\mathbf{U}'(m,l))\big) + \Phi\big(\lambda_4(\mathbf{C}'(m,l))\big)\right]. \quad (7)$$

In the encryption operation, the phase of the randomly selected row/ column of original image is added with the phase of the randomly selected row/ column of the carrier image and scaled by a factor of 0.5. In the decryption process, the magnitude and phase values of the encrypted image are separated. The phase values are scaled by a factor of 2 and subtracted from the phase values of the carrier image to retrieve the phase of the original image.

$$\Phi\big(\lambda_3(\mathbf{U}'(m,l))\big) = 2\Phi\big(\mathbf{V}(m,l)\big) - \Phi\big(\lambda_4(\mathbf{C}'(m,l))\big). \quad (8)$$

Finally the original image is reconstructed using the magnitude of encrypted image, which is nothing but the magnitude of the original image and modified phase and then taking IDFT.

C. Encryption by magnitude and phase manipulation

This method is essentially obtained by combining the two methods described above. The block diagram of the encryption part of this method is given in Fig. 4. Row wise 1-D DFT is performed on the original image to be encrypted. The magnitude of the original image is encrypted by magnitude manipulation and the phase of the original image is encrypted by phase manipulation as described earlier. The first row of the encrypted image is obtained by combining the modified magnitude and modified phase resulting from the first random selection. This process is continued for all the rows in the original image. The encrypted image in the spatial domain from the row wise operation is constructed by the IDFT operation. The resulting encrypted image is further subjected to one more level of encryption by taking column wise DFT on the encrypted image. It is to be emphasized at this stage that, there are in total four carrier images used in the encryption operation, two for row wise and two for column wise magnitude and phase manipulation and all are randomly selected from the set of stored images. Also note that, setting λ_1 and λ_2 same as λ_3 and λ_4, respectively, would reduce the decrypter complexity considerably.

The block diagram of the decryption part of the proposed encryption method by magnitude and phase manipulation is given in Fig. 5. In the decryption process first the column wise decryption of magnitude and phase is done by using the respective carrier images. The column wise decrypted image is further subjected to row wise decryption to obtain the original image.

IV. Experimental Results and Discussions

Gray level *lena* image is taken as the original image to be encrypted and the other images are chosen as carrier images. The original image, randomly chosen carrier image, their magnitude and phase spectra, modified magnitude spectra by the proposed magnitude manipulation method, resulting encrypted image and the corresponding decrypted image are shown in Fig. 6. As it can be observed from the figure, the encrypted image by the proposed magnitude manipulation is distorted and the decrypted image is free from any distortion.

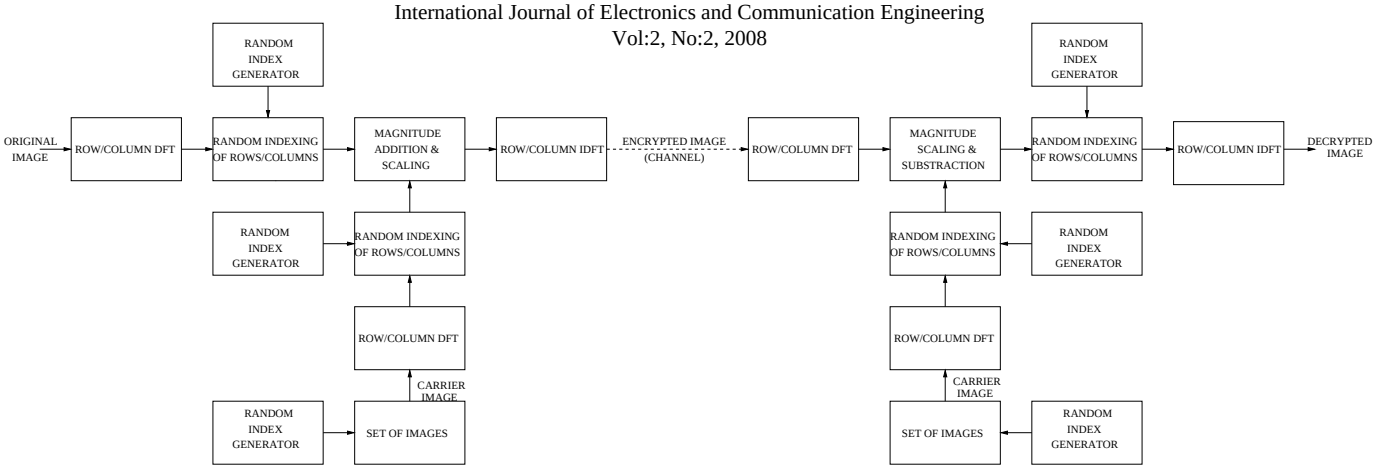

Fig. 3. Block diagram of encryption and decryption operations by magnitude manipulation method. For phase manipulation method, a similar treatment is carried out by substituting 'magnitude' with 'phase' in the above diagram.

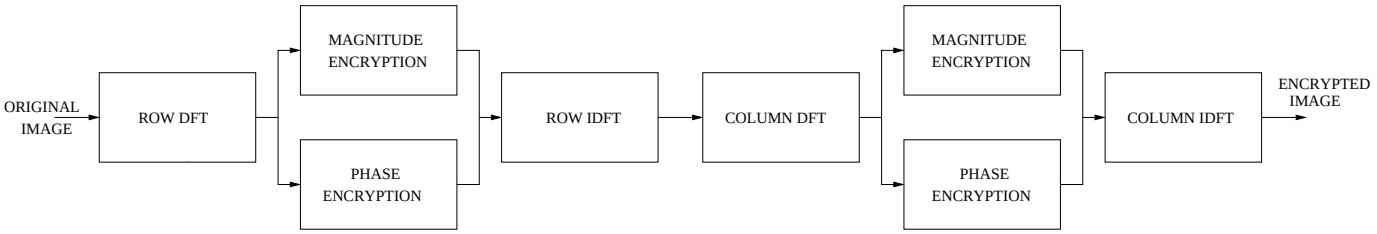

Fig. 4. Block diagram of encryption part of magnitude and phase manipulation method.

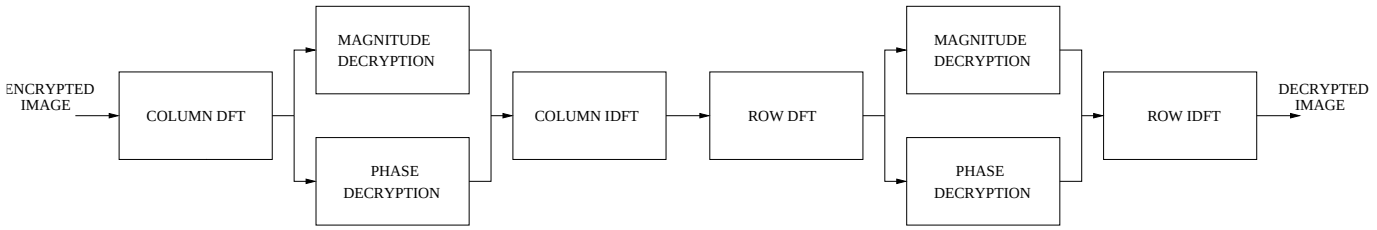

Fig. 5. Block diagram of decryption part of proposed magnitude and phase manipulation method.

The peak signal to noise ratio (PSNR) of the encrypted and decrypted images with respect to the original image is found to be 5.3 dB and 314.8 dB, respectively [20]. Lower the PSNR, more distorted will be the image and hence contains less information about the original image. By visual perception, we can observe that the encrypted image contains most of the information about the original image. The same set of images for the proposed phase manipulation method are shown in Fig. 7. As it can be observed from the figure, the encrypted message by the proposed phase manipulation method is fully distorted and the decrypted image is free from any distortions. The PSNR of the encrypted and decrypted images with respect to the original image is found to be 12.4 dB and 307.5 dB. By visual perception also, we can observe that the encrypted image does not contain much information about the original image.

The original image, randomly chosen carrier images, encrypted image by row wise encryption using magnitude and phase manipulation and encrypted image using row and then column wise encryption using magnitude and phase manipulation and their respective decrypted images are shown in Fig. 8. As it can be observed from the figure that the encrypted image by the proposed combined method is fully distorted and the decrypted image is free from any distortions. The PSNR of the encrypted and decrypted images with respect to the original image is found to be 11.9 dB, 11.9 dB, 11.9 dB and 301.7 dB, respectively. By visual perception also, we can observe that the encrypted image does not contain much

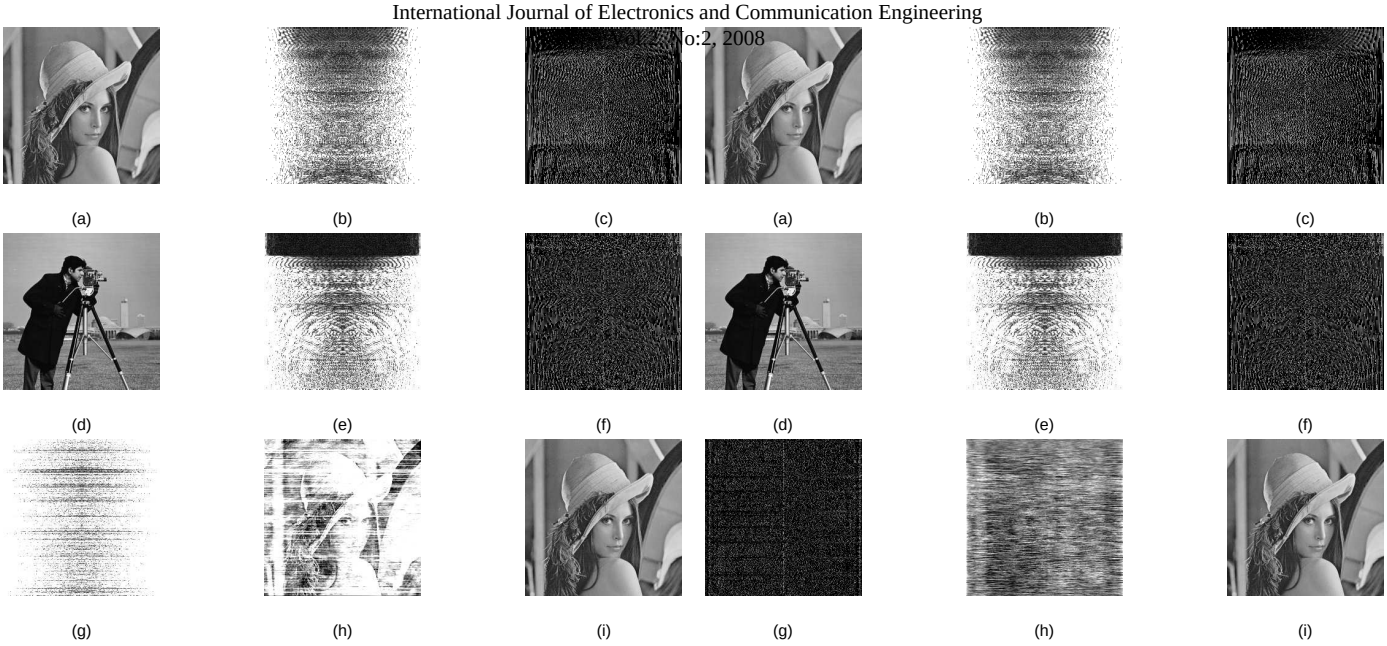

Fig. 6. Results of encryption by magnitude manipulation using carrier images. (a) Original image to be encrypted, (b) and (c) magnitude and phase spectra of original image, (d) carrier image, (e) and (f) magnitude and phase spectra of carrier image, (g) modified magnitude spectra, (h) encrypted image and (i) decrypted image.

Fig. 7. Results of encryption by phase manipulation using carrier images. (a) Original image to be encrypted, (b) and (c) magnitude and phase spectra of original image, (d) carrier image, (e) and (f) magnitude and phase spectra of carrier image, (g) modified phase spectra, (h) encrypted image and (i) decrypted image.

information about the original image. Further, Fig. 9 shows the effectiveness of the proposed method by changing the order of row and column wise operations at the receiver side, where the received image is totally garbled. Also, it can be observed from Fig. 6, 7 and 8, the magnitude manipulation method distorts the information in the original image to the least extent whereas the phase manipulation method as well as the combined method perform the same to a better extent. Further, the distortion in the phase manipulation method seem to be significant. This infers that the phase contains maximum information about the images [21]. From the PSNR and the complexity point of view the combined method seems to be preferable compared to individual manipulations.

The effectiveness of the proposed method, evaluated in terms of mean square error (MSE) and PSNR for different images, is tabulated in Table I. The entries in the table show the average values taken across several images. The relatively higher MSE and lower PSNR in case of combined magnitude and phase encryption method compared to either magnitude or phase encryption alone indicates that the combined method is preferable.

One important observation was made during the experimental studies. By visual observation, it can be seen that the encrypted image by magnitude manipulation is less distorted compared to that of phase manipulation and combined methods. Even though this behavior is reflected by MSE and PSNR in the average sense as given in Table I, it was observed in some cases that the PSNR of the encrypted image by magnitude manipulation is lower compared to that of the other two methods. Not that in such cases the pixel values in the encrypted image by magnitude manipulation are seen to be less near to original image than that by the other two methods. This may be the reason for low PSNR in case of magnitude manipulation compared to the other two.

TABLE I
PERFORMANCE OF PROPOSED IMAGE ENCRYPTION METHODS

Encryption	MSE	PSNR
Magnitude	1727.5	15.37
Phase	4521.3	11.37
Magnitude and Phase	4899.2	10.76

V. SUMMARY AND CONCLUSIONS

In this paper, we have proposed a method for encryption of images using carrier images, particularly with magnitude and phase manipulations. The proposed method is based on the fact that the individual components of a combined signal can be known only when all the carrier components are known, thereby increasing the security. From the experimental results we can infer that the combined magnitude and phase manipulation method provides full distortion in the encrypted image and also the method is computational intensive to break. Thus this method may be used in places where there is need to provide security against causal observers and also in tactical

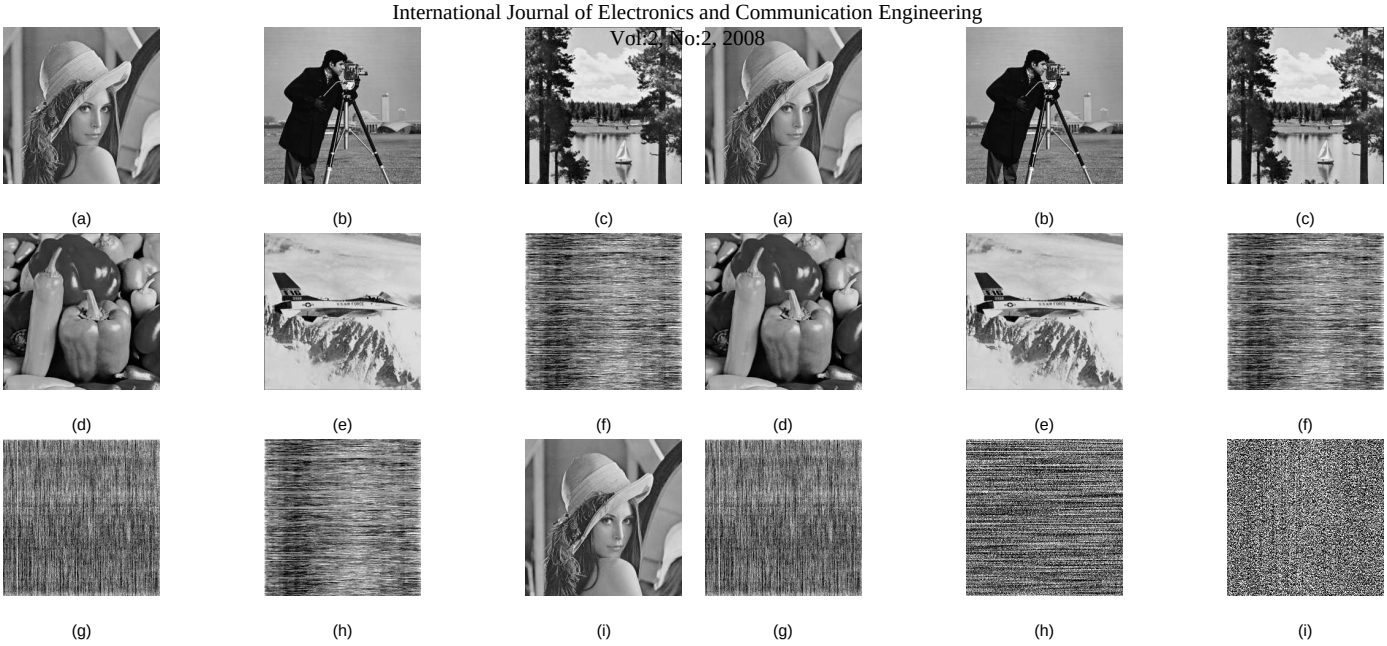

Fig. 8. Results of encryption by magnitude and phase manipulation using carrier images. (a) Original image, (b), (c), (d), (e) different carrier images, (f) encrypted image by row wise operation, (g) encrypted image by row and column wise operation, (h) decrypted image by column wise operation and (i) decrypted image by column and row wise operation.

Fig. 9. Efficiency of the proposed scheme. (a) Original image, (b), (c), (d), (e) carrier images, (f) encrypted image by row wise operation, (g) encrypted image by row and column wise operation, (h) decrypted image by row wise operation and (i) decrypted image by row and column wise operation.

applications where security is needed for short duration like few hours and days.

In the present work the proposed methods operate in the frequency domain. There are certain algorithms which operate in spatial domain too. These algorithms may also be effectively combined with the existing ones to provide better security.

REFERENCES

[1] H. J. Beker and F. C. Piper, *Cipher Systems: The Protection of Communications.* John Wiley & Sons, New York, 1982.

[2] C. P. Wu and C. J. Kuo, "Design of Integrated Multimedia Compression and Encryption Systems," *IEEE Trans. Multimedia*, vol. 7, no. 5, pp. 828-839, Oct. 2005.

[3] J. A. Buchmann, *Introduction to Cryptography.* Springer, New Delhi, 2004.

[4] O. Goldreich, *Foundations of Cryptography: Vol I Basic Tools.* Cambridge University Press, UK, 2005.

[5] O. Goldreich, *Foundations of Cryptography: Vol II Basic Applications.* Cambridge University Press, UK, 2005.

[6] K. S. Chan and F. Fekri, "A Block Cipher Crypto System using Wavelet Transforms over Finite Fields," *IEEE Trans. Signal Processing*, vol. 52, no. 10, pp. 2975-2991, Oct. 2004.

[7] S. Trivedi and R. Chandramouli, "Secret Key Estimation in Sequential Steganography," *IEEE Trans. Signal Processing*, vol. 53, no. 2, pp. 746-757, Feb. 2005.

[8] A. Martin *et. al.*, "Is Image Steganography Natural?," *IEEE Trans. Image Processing*, vol. 14, no. 12, pp. 2040-2050, Dec. 2005.

[9] K. Satish *et. al.*, "Chaos based Spread Spectrum Image Steganography," *IEEE Trans. Consumer Electronics*, vol. 50, no. 2, pp. 587-590, May. 2004.

[10] M. Ramkumar and A. N. Akansu, "Signaling methods for multimedia steganography," *IEEE Trans. Signal Processing*, vol. 52, no. 4, pp. 1100-1111, Apr. 2004.

[11] A. Takahashi *et. al.*, "Multiple Watermarks for Stereo Audio Signals using Phase-Modulation Techniques," *IEEE Trans. Signal Processing*, vol. 53, no. 2, pp. 806-815, Feb. 2005.

[12] F. H. Wang *et. al.*, "Hiding Watermark in Watermark," in *Proc. IEEE Int. symp. Circuits Syst.* (ISCAS), Kobe, May 23-26, 2005, pp. 4018-4021.

[13] V. Solachidis and L. Pitas, "Circularly Symmetric Watermark Embedding in 2-D DFT Domain," *IEEE Trans. Image Processing*, vol. 10, no. 11, pp. 1741-1753, Nov. 2001.

[14] I. J. Cox *et. al.*, *Digital Watermarking.* Morgan Kaufmann Publishers, CA, USA, 2002.

[15] H. J. Beker and F. C. Piper, *Secure Speech Communications.* Academic Press, London, 1985.

[16] O. Goldreich, *Foundations of Cryptography: Volume I Basic Applications.* Cambridge University Press, London, UK, 2005.

[17] O. Goldreich, *Foundations of Cryptography: Volume II Basic Tools.* Cambridge University Press, London, UK, 2005.

[18] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 118-129, Mar. 2003.

[19] S. Sridharan *et. al.*, "A fast fourier transform based speech encryption system," *Proc. IEE Communication, Speech and Vision*, vol. 138, no. 3, pp. 215-223, June 1991.

[20] A. K. Jain, *Fundamentals of Digital Image Processing*. Englewood Cliffs, NJ: Prentice Hall, 1989.

[21] A. V. Oppenheim *et. al.*, *Signals and Systems*. Englewood Cliffs, NJ: Prentice Hall, 1996.

[22] A. V. Oppenheim and R. W. Schafer, *Digital Signal Processing*. Englewood Cliffs, NJ: Prentice Hall, 1975.