IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

A Novel Approach for Security in Digital Image Processing Using Water Marking: Analysis

Prabhpreet Kaur[1*], Sonali Kanotra[2]

[1,2] G.N.D.U, Amritsar, India

Available online at: www.ijcseonline.org

Received: 20/Mar/2018, Revised: 28/Mar/2018, Accepted: 19/Apr/2018, Published: 30/Apr/2018

ABSTRACT -In this era of digital security, protection and illegal redistribution of digital media has become a major issue. The digital watermarking has been utilized to shield digital data from illicit redistribution and changes. In digital water denoting the image has been upgraded by installing commotion tolerant flag into transporter flag. Encryption procedures used to encode critical information has been inclined to assaults or attacks. Assist examination in encryption yields image encryption instrument as contrasting option to content encryption. The investigation of different system of digital watermarking as image encryption has been done in this paper to examine techniques which are better and can be used in future for enhancement; likewise the commitment of watermarking methods for security purposes has been broke down. The proposed literature provides comparative studies of techniques used in watermarking along with attributes considered including PSNR and MSE for enhancement.

Keywords: Digital Security, Watermarking, Encryption, PSNR MSE

1. INTRODUCTION

Image encryption provides essential characteristics to classified transmission of information over web. Image contains vast amount of information that requires significant testing for approval. Image encryption is generally accomplished in frequency, spatial and hybrid domain. The frequency domain security mechanisms include stegnography. [1]The stegnography is a successor of cryptography. Cryptography provides encryption of data which is being transmitted from source to destination.[2] The cryptography mechanism does not provide conceal to encrypted data hence chances of attack increases. The prime objective of stegnography is to conceal the features hence viability of attack decreases. Capacity of data which can be hidden within image using stegnography is vast along with robustness of stegnography provides unprecedented advantage over cryptography. Spatial domain considered pixel intensity values while encryption. Space is conserved hence bandwidth required in order to transfer the data from source to destination is reduced considerably. [3]Image stegnography included within spatial domain includes MSB stegnography. Most significant bits considered for encryption of text within image. Information is concealed and features are not visible that leads to high end security. Hybrid domain on the other hand provides mechanism using features of both spatial and frequency domains. Hybrid domain also uses application of watermarking to provide security against malicious attacks. Contrast and intensity values are altered to merge multiple images together. Key is generated for receiver to decode the text enclosed within the image. High end security is a result for watermarking.[4]The watermarking mechanism can be improved to provide low MSE(Mean square error) and high peak to signal ratio(PSNR). The capacity of information that can be transmitted through watermarking technique is vast. Chances of attack are maximized as the feature is exposed against the malicious users. The parameters that can be evaluated using watermarking techniques is as under:

1.1 MSE

[5]Mean square error(MSE) is evaluated in order to determine worth of technique. This parameter must be minimized. The equation used for evaluation of MSE is given as under

$$MSE = \sqrt{(X - X_i)^2 + (Y - Y_i)^2}$$

1.2 PSNR

[6]Peak signal to noise ratio parameter must be high and technique satisfying this condition is considered for future work. Equation used for PSNR is given as under

$$PSNR = \frac{Signal}{Noise}$$

The classification of information security techniques is given as under

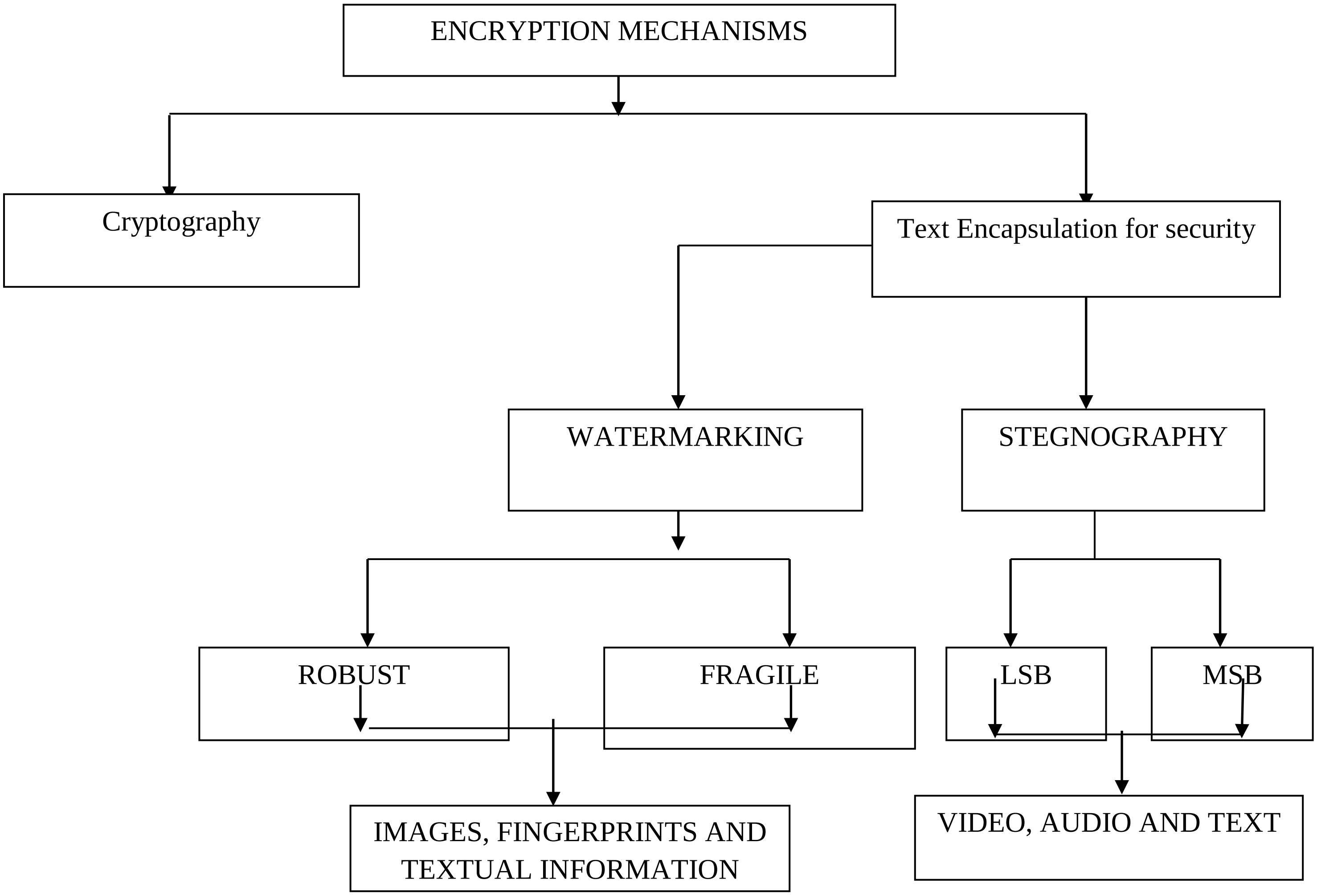

Figure 1: Classification of various security systems along with applications.

The paper is further is organized as under: Section II provides the literature review. Section III includes surveys on digital watermarking and contains comparison table of various techniques Section IV Research Gap Section V Conclusion.

2. RELATED WORK

Related work in the field of Image security is done to determine optimal techniques used to provide high capacity image transmission mechanism. The techniques are as discussed below

2.1 DISCRETE COSINE TRANSFORMATION(DCT)

[7]DCT is an effective mechanism that provides image encryption. DCT is used to convert image from spatial domain to frequency domain. DCT is applied at source end from where information is to be transferred. Inverse DCT is applied at destination end to decode the transmitted information. The equation used for encryption at source end is given as

$$F(x,y) = \frac{1}{4} * C(u)C(v) \sum \sum f(x,y) * \frac{\frac{\cos(2\pi x + 1)}{16} \cos(2\pi y + 1)}{16}$$

Where c indicates caricars used to transfer the signals f is a function indicating frequency domain, u and v indicates range of values that are required to be transmitted.

At the receiver end inverse DCT is applied as under

$$F(u,v) = \frac{1}{4} * C(x)C(y) \sum \sum f(u,v) * \frac{\frac{\cos(2\pi x + 1)}{16} \cos(2\pi y + 1)}{16}$$

2.2 STEGNOGRAPHY METHODS

[3], [8]Stegnography uses images to store the text to be transmitted. The transmitted image is decoded at the receiver end using a key. The extra image space is used to store text information to be transmitted. The technique of extra space preservation is associated with digital images. In LSB stegnography, the image encryption is performed at the bit levels. The pixel intensity values are altered during encryption. In case of distortion, tradeoff exists between payload and distortion. Payload vary as distortion appear within the image. This distortion is a part of attack. Filtering mechanism accompanied with stegnography. Filtering mechanisms enhances the peak signal to noise ratio and eliminate distortion if any present within the image. LSB stegnography is shown as under

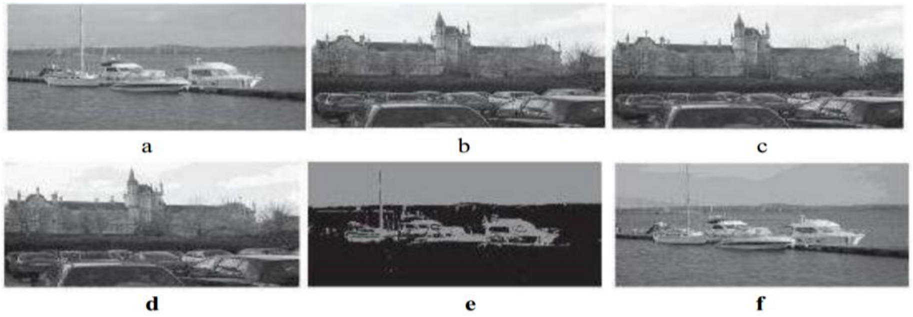

Figure 2: LSB Stegnography

An Image to be hidden b Carrier Image c First level of stegnography d Second level of stegnography e third level of stegnography f forth level of stegnography [9], [10]Stegnography in general involves replacement of nosy component within image with the random secret message. In stegnography most common noisy components are least significant bits (LSBs). These LSBs are imperceptible and hence can be replaced by secret messages.

Most significant bits also contains some noisy components and hence they can also be used to encode secret messages. The perpotion of image encryption is limited as compared to LSB stegnography. The MSB stegnography can replace LSB stegnography in case data to be transmitted is limited in quantity.

2.3 WATERMARKING

[11], [12]Watermarking is another mechanism used to provide image encryption. Contrast levels are varied within watermarking techniques to encode information within the image. There exist a primary image also known a carrier image and other image that contains information to be transmitted known as secondary image or logo. The contrast levels of primary image is reduced to certain degree and secondary image is merged using pixel encoding mechanism. the image so obtained is known as watermarked image. The watermarked image is then transmitted from source towards destination.

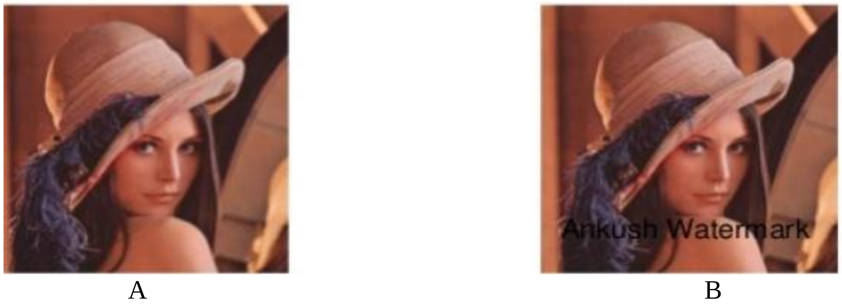

Figure 3: A Before watermarking B After Watermarking

Watermarking mechanism conceal the information features hence there are less chances of attack. Malicious activity is forbidden by the use of watermarking mechanism.

2.4 PCA

[13], [14]Principal Component analysis is simpler as compared to watermarking and stegnography. The principal component analysis is used to divide the image into viable and non viable components. The viable components features are extracted and analyzed. The viable components are formed through the matrix. The critical information is lost during this transformation. The size of image is reduced significantly. PCA approach alone however may not give optimal results. The matrix representation associated with the image encryption is as under

$$Y_{Mxn^2} \left| \begin{matrix} v_1 - - - v_m \\ v_n - - - v_{nm} \end{matrix} \right| * \left] \begin{matrix} X_i - - - - X_m \\ Xm - - - Xmn \end{matrix} \right] - \left[\begin{matrix} m_1 - - - - m_n \\ m_m - - - - m_{mn} \end{matrix} \right]$$

The critical components when extracted information is lost. The intensity values of pixel is significantly reduced. This affect is represented through the following image segments

Figure 4: Before applying PCA

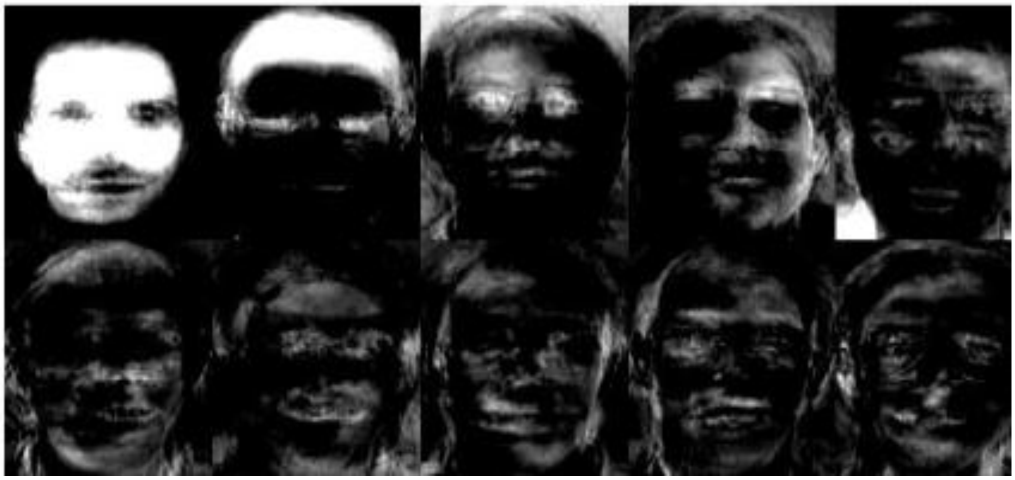

Figure 5: After Applying PCA

Features are extracted and critical information is lost. The size is reduced considerably and can be used in an area where bandwidth is limited.

2.5 COMPARISON OF TECHNQIUES USED FOR IMAGE SECURITY

Author	Title	Dataset/Image Type	Journal/Conference	Technique	Parameters	Merits	Demerits
M. Sajid et. Al	[15]Image Encryption using Different Techniques for High Security Transmission over a Network	JPEG images are used for Encryption	IEEE	Hexadecimal Encryption	Key size Time consumption	More secure since sixteen distinct keys are used for encryption	It takes more time for encryption and transmission
T. Zhang et.Al	[16] A New Combined Chaotic System for Image Encryption	JPEG image set is used for chaotic encryption	IEEE	Chaotic Encryption	Entropy Key size	Chaotic Maps provide more security as compare to cryptography	Time consumption and entropy can be further optimized
A. Elsayed et.Al	[17] Highly Secure Image Steganography Algorithm using Curvelet Transform and DCT Encryption	JPEG image with 640x480 as cover and 250x250 image as logo image	IEEE	Stegnography using DCT	Image Size MSE	Mean Square error is reduced and image size is also reduced	More text cannot be encrypted within the image
Y. Zhou et. Al	[18] Image Encryption Using Binary Key-images	BMP file are used for encryption	IEEE	Binary image key	Key Size Image size	Complex key ensure security of data	Time consumption in image encryption is high
A. U. Islam et.Al	[10] An Improved Image Steganography Technique based on MSB using Bit Differencing	JPEG images for cover and logo images	INTECH	MSB stegnography with Bit differencing	PSNR Payload	Peak signal to noise ratio is increased and payload is reduced	Complexity and time consumption is high. MSE is not considered which is also high in this case.
xiaolin wu et. Al	[19] A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps	JPEG image set	IEEE	Chaotic tent Map	Image Key size	Image key size is large and hence security is improved	Time complexity is enhanced
A. Belazi et. Al	[20] A novel image encryption scheme based on substitution-permutation network and chaos	JPEG images used for encryption	IEEE	Substitution Cipher	Key size Security Speed	High Security, Speed and key size is accomplished	It can be implemented using network protocols only
M.	[21] Spatial Domain	JPEG imageset	IEEE	Spatial domain	MSE	MSE is reduced	Capacity of text

Sandilya et. Al	Image Steganography based on Security and Randomization	used for encryption		Stegnography	PSNR Capcaity	PSNR is improved	information that can be encrypted need improvement
Z. Beiji et. Al.	[22] Information Security Technique in Frequency Domain	JPEG and PNG images can be used for encryption	IEEE	DCT	MSE	MSE is reduced	PSNR can be further improved
M. Mofarreh-bonab et. Al.	[23] Image Encryption by PCA	JPEG image encryption	IEEE	PCA	Contrast improvement	Contrast improvement is achieved	MSE and PSNR needs to be optimised

Table 1: Comparison of techniques used for image encryption

3. RESEARCH GAP

The image security concerns are an issue required to be tackled in the future endeavour. The exiting techniques focus on image encryption which is exceeding oriented towards key. The image encryption in which image is encoded within another image to enhance PSNR and MSE in future work. The PSNR and MSE in existing mechanism not optimized. The image decomposition mechanism can be enforced in future work to reduce complexity of image.

4. CONCLUSION AND FUTURE SCOPE

Information transferred through web is always at stakes due to high degree of malicious activities present. In order to overcome the problem security mechanism are devised. Cryptography is preferred for performing encryption and making secure communication among source and destination. Information conceal is required so that features are not disclosed to prevent attack. Unfortunately this information conceal to hide feature is poor in case of cryptography. In order to resolve the problem, image encryption is used. Image encryption through watermarking provide scope since MSE and PSNR are optimized by the use of this encryption mechanism.

In future, watermarking with DCT can be explored for encryption to enhance PSNR and reduce MSE.

REFERENCES

[1] X. Pan, B. T. Yan, and K. Niu, “Multiclass detect of current steganographic methods for JPEG format based re-stegnography,” Link: http://www.ws.binghamton.edu/fridrich/Research/single.pdf , *Proc. - 2nd IEEE Int. Conf. Adv. Comput. Control. ICACC 2010*, vol. 4, no. experiment 1, pp. 79–82, 2010.

[2] R. Gupta and T. P. Singh, “New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters,” doi: 10.1109/IIH-MSP.2013.134 *Proc. 2014 Int. Conf. Contemp. Comput. Informatics, IC3I 2014*, pp. 475–479, 2014.

[3] X. Pan, B. Yan, and K. Niu, “Multiclass Detect of Current Steganographic Methods for JPEG Format Based Re-stegnography,”doi: 10.1109/ICCIAS.2006.295451, IEEE Access ,no. experiment 1, pp. 2–5, 2014.

[4] N. Sarani and K. Amudha, “A security technique based on watermarking and encryption for medical image,” doi: 10.1109/ICIIECS.2015.7192934, *ICIIECS 2015 - 2015 IEEE Int. Conf. Innov. Information, Embed. Commun. Syst.*, pp. 3–6, 2015.

[5] M. Mese and P. P. Vaidyanathan, “Optimal histogram modification with MSE metric,” doi:10.1109/ICIIECS.2015.7192934 in *2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No.01CH37221)*, 2001, vol. 3, pp. 1665–1668, 2001.

[6] C. Chang-yanab, Z. Ji-xian, and L. Zheng-jun, “Study on methods of noise reduction in a stripped image,” doi: 10.1109/TGRS.2016.2594080 *IEEE Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.*, no. 1, pp. 2–5, 2008.

[7] A. Kaur and J. Kaur, “Comparision of Dct and Dwt of Image Compression Techniques,” Doi: 10.1109/IPAS.2016.7880068 vol. 1, no. 4, pp. 49–52, 2012.

[8] K. Saranya and A. Professor-i, “Modern Applications of QR-Code for Security,” DOI: 10.1109/ICETECH.2016.7569235 no 2. March, pp. 1–5, 2016.

[9] V. Saravanan and A. Neeraja, “Security issues in computer networks and stegnography,” DOI: 10.1109/ISCO.2013.75696 *7th Int. Conf. Intell. Syst. Control. ISCO 2013*, pp. 363–366, 2013.

[10] A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali, and M. Naeem, “An improved image steganography technique based on MSB using bit differencing,” DOI: 10.1109/INTECH.2017.6935,*2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016*, pp. 265–269, 2017.

[11] T. Bathinda, “Invisible Video Multiple Watermarking Using Optimized Techniques,” doi: 10.1129/IEEE.2016.7929 IEEE Access vol. 3, pp. 1665–1668, 2016.

[12] S. S. Gonge, “An Integration of SVD Digital Image Watermarking with AES Technique for Copyright Protection and Security of Bank Cheque Image,”DOI: 10.12109/IEEE.2016.192934, IEEE pp. 769–778, 2016.

[13] P. Peng and I. S. Member, “Efficient Face Verification in Mobile Environment Using Component-based PCA,” doi: 10.12023/CISP.2013.71934no.3 Cisp, pp. 753–757, 2013.

[14] V. Ponomaryov, “Computer-aided detection system based on PCA/SVM for diagnosis of breast cancer lesions,” doi: 10.1102/CCEEEC.2015.12304,*2015 Chil. Conf. Electr. Electron. Eng. Inf. Commun. Technol.*, pp. 429–436, 2015.

[15] M. Sajid, Q. Khizrai, and P. S. T. Bodkhe, “Image Encryption using Different Techniques for High Security Transmission over a

Network,”DOI: 10.1209/IEEE.2014.34294 IEEE access vol. 2, no. 4, 2014.

[16] T. Zhang, Y. Zhou, and C. L. P. Chen, “A new combined chaotic system for image encryption,” doi: 10.1109/CSAE.2012.45923342,*CSAE 2012 - Proceedings, 2012 IEEE Int. Conf. Comput. Sci. Autom. Eng.*, vol. 2, no. 2, pp. 331–335, 2012.

[17] A. Elsayed, A. Elleithy, P. Thunga, and Z. Wu, “Highly secure image steganography algorithm using curvelet transform and DCT encryption,” DOI: 10.1109/IEEE.2015.342934*2015 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2015*, pp. 2–7, 2015.

[18] Y. Zhou, K. Panetta, and S. Agaian, “Image encryption using binary key-images,” DOI: 10.1119/IEEE.2009.5602934 *2009 IEEE Int. Conf. Syst. Man Cybern.*, no. October, pp. 4569–4574, 2009.

[19] xiaolin wu, B. Zhu, Y. Hu, and Y. Ran, “A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps,” DOI: 10.1219/IEEE.2017.100986,*IEEE Access*, vol. 3536, no. c, pp. 1–1, 2017.

[20] A. Belazi, A. A. Abd El-Latif, and S. Belghith, “A novel image encryption scheme based on substitution-permutation network and chaos,”DOI: 10.23109/IEEE.2015.7192934,IEEE *Signal Processing*, vol. 128, pp. 155–170, 2016.

[21] M. Sandilya and M. Chawla, “Spatial Domain Image Steganography based on Security and Randomization,” DOI:11.4564/IEEE.2014.674934IEEE ACCESSvol. 5, no. 1, pp. 156–159, 2014.

[22] Z. Beiji and M. Y. Abdullah, “Information Security Technique in Frequency Domain,”, DOI: 10.5673/IACS.2011.234094 IEEE ACCESS vol. 5, no. December, pp. 279–289, 2011.

[23] M. Mofarreh-bonab, “Image Encryption by PCA,”DOI: 10.2239/IEEEOCS.2015.543623 IEEE OPEN ACCESS vol. 3, no. 3, pp. 28–30, 2015.