Development of Robust-Secure Data Hiding Technique for Color Images

M.A. Mohamed[1], M.E.A. Abou-ElSeoud[2] and Islam .M. Ibrahim[3]

**[1] ECE, Mansoura University, Faculty of Engineering
Mansoura, Dakhlia, Egypt**

**[2] ECE, Mansoura University, Faculty of Engineering
Mansoura, Dakhlia, Egypt**

**[3] ECE, Mansoura University, Faculty of Engineering
Mansoura, Dakhlia, Egypt**

Abstract

The paper proposed a secure technique for color images using DCT-DWT technique and AES-128 bit Key encryption algorithm for improving security of system. Host image converted to YIQ after embedding using DWT. The quality of watermark measured by metrics such as; structural similarity (SSIM) and quaternion structural similarity (QSSIM).This improves traditional methods. Experimental results proved that this technique is robust for attacks.

Keywords: *DCT-DWT-YIQ, watermark, AES, Histogram, SSIM.*

1. Introduction

Watermarking introduce high encrypted data. It is better method of cryptography .Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications. The majority of work done on watermarking recently uses frequency domain. The frequency domain techniques are more popular than spatial domain techniques because working in this domain produces more robust and imperceptible watermarking. Whether using spatial domain or frequency domain, the image is converted to any of these respective domains before embedding the watermark. In spatial domain, the watermark Image is embedded on the whole cover image pixels directly [5]. Encryption is the process of transforming information (plaintext) using an algorithm (cipher) to make it unreadable to anyone except those possessing authorization. The result of this process is an output cipher text. Secret key encryption uses a common key to encrypt or decrypt the message. Public key encryption, known as a symmetric encryption which uses two different keys such as a public key known by all and a private key known only by the sender and the receiver.

Advanced Encryption Standard (AES) is a symmetric block cipher and became the designated successor of the Data Encryption Standard (DES) [13]. Watermarking is a process which embeds data into digital contents such as text, images, video and audio without degrading the overall quality of the digital media. The possible domain for watermark embedding is that of the wavelet domain. The Discrete Wavelet Transform (DWT) separates an image into a lower resolution approximation image (LL), horizontal (HL), vertical (LH) and diagonal (HH) detail components.

2. Background & Related Works

Much software which can be used to download picture contents from the internet, quickly and with ease, is free; and is readily available. Watermarking which is a solution to this problem has been proposed by many researchers. Though continuous wavelet transform is available in transform domain, but have its own limitations. Discrete Wavelet Transform provides multi resolution for image and can implemented using digital filter; it has become attraction of researchers in image processing area. Here, review of literature survey is done on different transform in transform domain and existing color image watermarking techniques based on Discrete Wavelet Transform DWT. The Following methods are for in color image watermarking: Integer Wavelet Transform with Bit Plane complexity Segmentation is used with more data hiding capacity. This method used RGB color space for watermark embedding. In [5] DWT based watermarking algorithm of color images is proposed. The RGB color space is converted into YIQ color space and watermark is embedded in Y and Q components. RGB color space can be converted into YIQ color space. Y' is similar to perceived luminance; 'I and Q' carry color information and some luminance information.

Since pixel values are highly correlated in RGB color spaces, the watermark embedding in YIQ color space is preferred for Watermarking. Initially color image is read and R, G; B components of original Cover Image are separated.
Then they are converted into YIQ color Space using following equations [3]. After conversion of RGB color spaces into YIQ color spaces, Watermark is embedded [2].

$$Y = 0.299 * R + 0.587 * G + 0.114 * B \quad (1)$$
$$I = 0.596 * R - 0.274 * G - 0.322 * B \quad (2)$$
$$Q = 0.211 * R - 0.522 * G + 0.311 * B \quad (3)$$

After embedding the watermark using DWT, YIQ color space is converted back into RGB color
Space using following equations:

$$R = Y + 0.956 * I + 0.621 * Q \quad (4)$$
$$G = Y - 0.272 * I - 0.647 * Q \quad (5)$$
$$B = Y- 1.106 * I + 1.702 * Q \quad (6)$$

This method gives correlation up to 0.91 in JPEG Compression attack. In [3], Watermarking Algorithm Based on Wavelet and Cosine Transform for Color Image is proposed. A binary image as watermark is embedded into green or blue component of color image. Color Image watermarking algorithm based on DWT-SVD is proposed. The scrambling watermark is embedded into green component of color image based on DWT-SVD. The scheme is robust and giving PSNR up to 42, 82. In [5], Pyramid Wavelet Watermarking Technique for Digital Color Images is proposed. This algorithm gives better security and better correlation in Noise and compression attacks. Many research works are developed for encryption and watermarking based authentication. The algorithm proposed is based only on JPEG2000 compressed code streams, since the embedding is done in the compressed ciphered byte streams. The embedding position plays a crucial role in deciding the watermarked image quality. New hybrid approach of encryption-compression is proposed. This is based on the AES encryption algorithm and compression, in which image quality is lost due to compression of the input data. The encryption is performed on most significant bit planes while watermarking the rest of lower significant bit planes. Suppose if lesser number of bit planes are used for encryption, an attacker can easily manipulate the un-encrypted bit planes and further extract some useful information from the image which leads to loss in image quality. The addition or subtraction of a watermark bit to a sample is based on the value of quantized plaintext sample. However, in our algorithm, the watermark embedder does not have access to the plain text values as they have only the encrypted content. Also the watermark embedders don't have the key to UN-encrypt the plain text values to embed the watermark. Thus, watermarking in encrypted domain is very challenging.

3. Watermarking Embedding algorithm

The block diagram of the proposed technique shown in Figure1. The input image to be transmitted is separated into wavelet sub-bands using 1-level haar transform. AES Encryption algorithm is proposed to encrypt the LL sub band and Block DCT based watermarking algorithm is used to embed binary watermark in LH sub-band. Generally, frequency-based techniques are very robust against attacks like compression and filtering because the watermark is generally spread throughout image. So, to obtain better imperceptibility and also robustness, the addition of the watermark is done in a transformed domain. Inverse DWT is used for obtaining the Encrypted Watermarked image which is to be transmitted at the transmitter side. At the receiver side, watermark recovery and decryption is performed in respective sub-bands [5].

Step 1: Read Host Image of 512x512 sizes. Separate its R, G, B components and convert into YIQ color. Space using equations 1, 2, 3.
Step 2: select I component and apply one level IDWT Consider HL1 sub band.
Step 3: watermark (RGB) with size 256x256 and converted to grey scale image.
Step 4: Read grey scale watermark of 256x256 sizes.
Step 5: Apply DCT after doing encryption.
Step 6: Depending upon key K1 we use AES.
Step 7: Apply inverse DWT with ‘LL1, New_HL1, LH1, HH1’ to get ‘New I’ component.
Step 8: Combine, Y, New I and Q components and convert to RGB color space using equation 4, 5, 6.

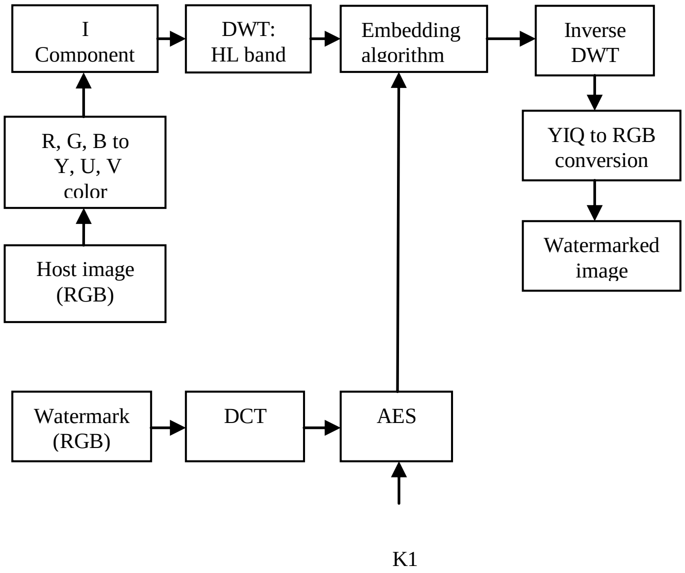

Fig. 1 watermark embedding algorithm

https://doi.org/10.20943/01201701.3540

4. Watermarking Extracting algorithm

Step 1: Read Color ‘Watermarked Image’ and separate it’s R, G and B components. Now
Convert to YIQ color space.
Step 2: Now select I component and apply one level DWT to retrieve HL1 sub band.
Step 3: Extract mid band elements from DCT block and find correlation between ‘extracted mid Band coefficients.
Step 4: Apply inverse DCT after encryption process.
Step 5: applying AES encryption algorithm.
Step 6: apply inverse DCT, then obtained final watermark (grey scale image).

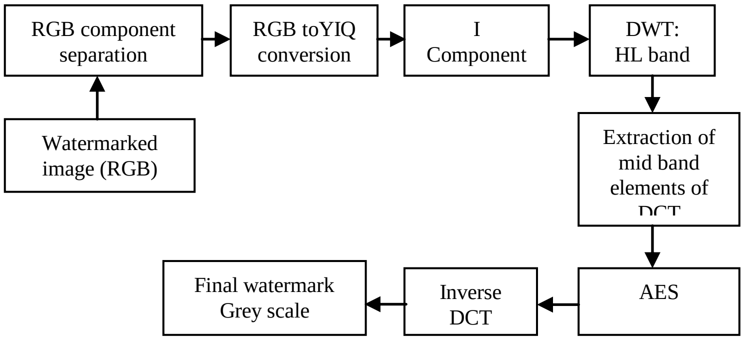

Fig. 2 watermark extracting algorithm

5. Results and Discussions

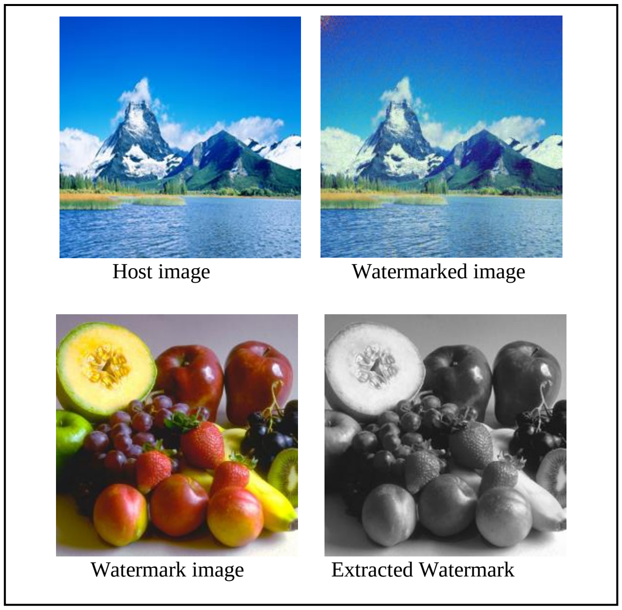
Host image
Watermarked image
Watermark image
Extracted Watermark

Fig. 3 Host , watermarked , watermark and Extracted Watermark image

The host image (RGB) image with size 512x512 converted to YIQ image . select I componenet and apply DWT (HL1) band.The watermarked image.watermark image (RGB) should converted first to greyscale image and apply discrete cosine transform DCT before encryption(i.e watermark should be greyscale not RGB before embedding and before DCT).The extracted watermark (greyscale image) so the watermark is embedded as a greyscale image and extracted also greyscale.

Table 1: Experimental results for measuring metrics to host image and watermarked image.

Host image&watermarke -d image	***Max***	***Min***	***Mean***	***STD***
SSIM	0.9019	0.4041	0.7147	0.0844
QSSIM	0.8953	0.3350	0.6515	0.1170
PSNR	14.3459	12.5664	13.3010	0.3175
MSE	1.0e+03 * 3.6012	2.3905	3.0488	0.2203
Correlation coefficient	0.9962	0.9018	0.9903	0.0072

Table 2: Experimental results for measuring metrics to original watermark and extracted watermark

Original watermark&extra-cted watermark	***Max***	***Min***	***Mean***	***STD***
SSIM	1	1	1	0
PSNR	Inf	Inf	Inf	NaN
MSE	0	0	0	0
Correlation coefficient	1	1	1	0

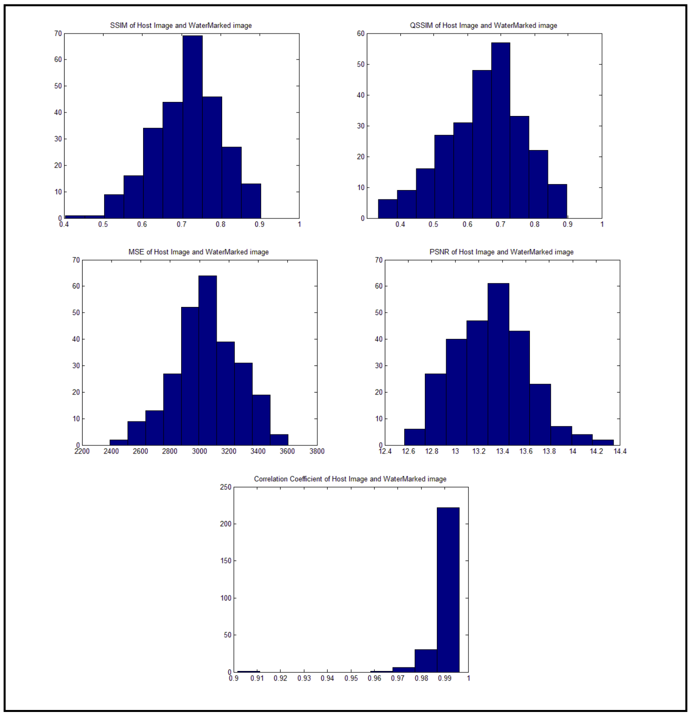

Fig. 4 SSIM, QSSIM, MSE, PSNR, Correlation coefficient of host and watermarked image

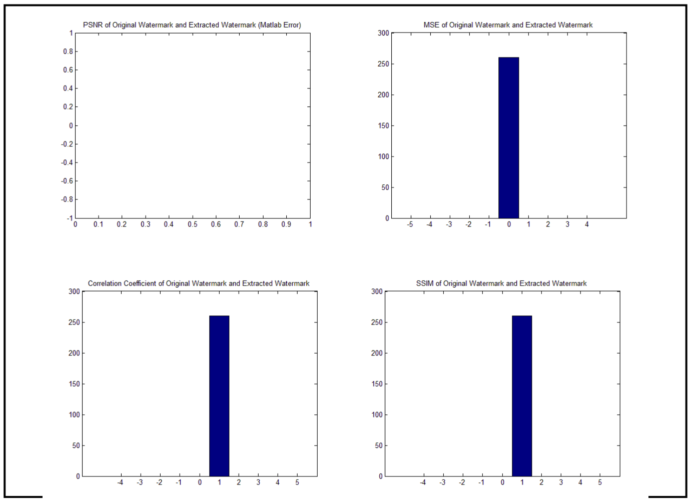

Fig. 5 PSNR, MSE, Correlation coefficient, SSIM of original and extracted watermark

5.1 Metrics

The quality of watermarked image is studied with peak signal to noise ratio (PSNR). Watermark image quality is analyzed using Normalized Correlation (NC) between the extracted and the original watermark.

PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [1].Peak Signal to Noise Ratio is calculated by the following formula: PSNR in decibels (dB) is represented as shown:

$$PSNR = 20\log\frac{MAX}{\sqrt{MSE}}$$

$$PSNR = 20\log\frac{MAX}{\sqrt{\frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X\left(i,j\right)\right)-\left(X'(i,j\right)^{2}}} \quad (7)$$

Where:

MSE: is the mean square error between the original image and the watermark image.

MAX**:** is the maximum pixel value of the image which is equal to 255 in our implementations since pixels were represented using 8 bits per sample.

$$\sigma_X = \left(\frac{1}{N-1}\sum_{i=1}^{N}((x_i-\mu_X)^2\right)^{\frac{1}{2}} \quad (8)$$

Where:
(M, N) are the image dimensions,
X (i, j) is the pixel value of original (host) image
X'(i, j) is the pixel value of the watermark image.
The correlation factor measures the similarity between the original watermark and the watermark extracted from the attacked watermark image (robustness). It take values between 0 (random relationship) to 1 (perfect linear relationship). The correlation factor is computed using Eq. shown:

$$R_{XY} = \frac{\sum_{i=1}^{n}(x_i - X')(Y_i - Y')}{\sqrt{\sum_{i=1}^{n}(X_i - X')^2\sum_{i=1}^{n}(Y_i - Y')^2}} \quad (9)$$

Where:
(N) is number of pixel of the image,
(Xi) is the pixel value of the original image,
(X) is the average of all pixels value of the original image
(Yi) is the pixel value of the modified image
(Y) Is the average of all pixels value of the modified image.

https://doi.org/10.20943/01201701.3540

In [22], The Structural Similarity (SSIM) Index We constructs a specific example of a structural similarity quality measure from the perspective of image formation. SSIM is used for measuring the similarity between two images. The SSIM index is a full reference metric; in other words, the measurement or prediction of image quality is based on an initial uncompressed or distortion-free image as reference. SSIM is designed to improve on traditional methods such as peak signal-to-noise ratio (PSNR) and Mean squared error (MSE), which have proven to be inconsistent with human visual perception. The SSIM index is calculated on various windows of an image. The measure between two windows and of common size N×N is:

$$SSIM((x,y)==\frac{(2\mu_x\mu_y+C1)(2\sigma_{xy}+C2)}{(\mu^2{}_x+\mu^2{}_y+C1)(\sigma^2{}_x+\sigma^2{}_y+C2)} \qquad (10)$$

Where:

(μ_x) The average of x

(μ_y) The average of y

($\sigma^2{}_x$) The variance of x

($\sigma^2{}_y$) The variance of y

(σ_{xy}) The covariance of x and y

$C1=(k_1L)^2$, $C2=(k_2L)^2$ Two variables to stabilize the division with weak denominator;
(L) The dynamic range of the pixel-values.
K1=0.01and K2=0.03
The mean intensity

$$\mu_X=\frac{1}{N}\sum_{i=1}^{N}(x_i-\mu_X)^2)^{\frac{1}{2}} \qquad (11)$$

The standard deviation (the square root of variance) as an estimate of the signal contrast. An unbiased estimate
In discrete form is given by

$$\sigma_X=(\frac{1}{N-1}\sum_{i=1}^{N}((x_i-\mu_X)^2)^{\frac{1}{2}} \qquad (12)$$

6. Conclusions

In this paper, a robust-secure data hidden technique is proposed to embed the watermark in encrypted image for color images using DCT-DWT domain. We used AES algorithm to improve the security of system. The proposed method also prevents the confidentiality of content since encryption is combined with watermarking. Measuring structural similarity (SSIM) and QSSIM improved PSNR and MSE.The use of YIQ color space for watermark embedding is better to improve the results. The images having difference histogram shapes that reflect better effect of this technique.

References

[1] Kunal D Megha1, Nimesh P Vaidya2, Asst. Prof Ketan Patel, Digital Watermarking: Data Hiding Techniques using DCT-DWT Algorithm, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2013.

[2]V.Chandra Prasad S.Maheswari, ROBUST WATERMARKING OF AES ENCRYPTED IMAGES FOR DRM SYSTEMS, PG Scholar, Department of EEE Assistant Professor, Department of EEEKongu Engineering College, Erode-638052, India Kongu Engineering College, Erode-638052, India, 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013)

[3]Baisa L. Gunjal1 and Suresh N.Mali SECURED COLOR IMAGE WATERMARKING TECHNIQUE IN DWT-DCT DOMAIN, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.3, August 2011

[4]S.Radharani1, Dr. M.L. Valarmathi, CONTENT BASED WATERMARKING FOR COLOR IMAGES USING TRANSFORM DOMAIN, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1,Jan-Feb 2012, pp.773-779.

[5]Ghazali Bin Sulong , Harith Hasan(Corresponding author) , Ali Selamat3 , Mohammed Ibrahim and Saparudin, A New Color Image Watermarking Technique Using Hybrid Domain,IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012.

[6] Jamal Ali Hussein, Sulaimani, Iraq, Luminance-based Embedding Approach for Color Image Watermarking, I.J. Image, Graphics and Signal Processing, 2012, 3, 49-55 .

[7] Vikas Saxena, Aditi Harsulkar, Performance Analysis of Color Channel for DCT Based Image Watermarking Scheme, International Journal of Security and its Applications Vol. 1, No. 2, October, 2007.

[8] Ibrahim Alsonosi Nasir, Member, IAENG, Ahmed b. Abdurrman, A Robust Color Image Watermarking Scheme Based on Image Normalization, Proceedings of the World Congress on Engineering 2013 Vol III, WCE 2013, July 3 - 5, 2013, London, U.K.

[9] D. Dia, M. Zeghid, M. Atri, B. Bouallegue, M. Machhout and R. Tourki, DWT-AES Processor for a Reconfigurable Secure Image Coding, International Journal of Computer Theory and Engineering, Vol. 1, No.2, June 2009.

[10] R. Eswaraiah, Sai Alekhya Edara, E. Sreenivasa Reddy, Color Image Watermarking Scheme using DWT and DC Coefficients of R, G and B Color Components, International Journal of Computer Applications (0975 8887)Volume 50 – No.8, July 2012.

[11] Supriya S. Sonawane, High Capacity Data Embedding Technique for Separable Encrypted Data Embedding in Encrypted Image, he International Journal of Science & Technoledge (ISSN2321 –919X), 2014.

[12] Md.Maklachur Rahman [17] A DWT,DCT AND SVD BASEDWATERMARKINGTECHNIQUETOPROTECTTHEIMAGE PIRACY, International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT)Vol. 4, No. 2, June 2013.

[13] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, New Comparative Study Between DES, 3DES and AES within Nine Factors , JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617.

[14] Vinsa Varghese1, Ragesh G.K21MTech Scholar, Dept. of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology, Kalady,Kerala, India, A SECURE METHOD FOR HIDING SECRET DATA ON CUBISM IMAGE USING HYBRID FEATURE DETECTION METHOD, IJRET: International Journal of Research in Engineering and TechnologyeISSN: 2319-1163 | pISSN: 2321-7308.

[15] GurpreetKaur, Kamaljeet Kaur, Digital Watermarking and Other Data Hiding Techniques, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013.

[16] R.Meenaksh, Dr.K.Kuppusmay, International Journal of Advanced Research in Computer Science and Software
Engineering, © 2014, IJARCSSE All Rights Reserved Page | 1047Volume 4, Issue 6, June 2014 ISSN: 2277 128X.

[17] Baisa L. Gunjal1 and Suresh N.Mali21Amrutvahini College of Engineering, Sangamner, A’nagar, MS, India, 2Imperial College of Engineering and Research, Wagholi, Pune, MS, India, SECURED COLOR IMAGE WATERMARKINGTECHNIQUE IN DWT-DCT DOMAIN, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.3, August 2011.

[18] 1Anjana Gupta, 2Mukesh Pathela, 1,2Uttarakhand Technical University, Dehradun, Uttarakhand, India, Performance Analysis of DWT-SVD-AES Watermarking, IJECT Vol. 7, Issue2, April - June2016.

[19] Ashwini B,Pushpalatha S, R H Goudar, A Hybrid Approach for Enhancing Data Security by Combining Encryption and Steganography, Proc. of the Intl. Conf. on Advances In Engineering And Technology-ICAET-2014Copyright © Institute of Research Engineers and Doctors. All rights reserved.ISBN: 97-1-63248-028-6 doi: 10.15224/ 9781-63248-028-6-01-19.

[20] R.Meenaksh, Dr.K.Kuppusmay, International Journal of Advanced Research in Computer Science and Software
Engineering, © 2014, IJARCSSE All Rights Reserved Page | 1047Volume 4, Issue 6, June 2014 ISSN: 2277 128X.

[21] E. Thambiraja, G. Ramesh, Dr. R. Umarani, A Survey on Various Most Common Encryption Techniques, 128XInternational Journal of Advanced Research in Computer Science and Software Engineering. © 2012, IJARCSSE All Rights Reserved Page | 226Volume 2, Issue 7, July 2012ISSN: 2277.

[22] Zhou Wang, Member, IEEE, Alan C. Bovik, Fellow, IEEE
Hamid R. Sheikh, Student Member, IEEE, and Eero P. Simoncelli, Senior Member, IEEE, Image Quality Assessment: From Error Visibility to Structural Similarity, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 13, NO. 4, APRIL 2004.

Mohamed Abdel-Azim Received the PhD degree in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2006. After that he worked as an assistant professor at the Electronics & Communications engineering department and now the head of at the Electronics & Communications engineering department. He has 51 publications in various international journals and conferences. His current research interests are in multimedia processing, wireless communication systems, and Field Programmable Gate Array (FPGA) applications.

Islam Mohammed Received the BSC degree in Electronics and Communications engineering- by 2011. After that he worked as a teaching assistant at the Electronics & Communications engineering department at the obour higher institute for engineering and technology-Cairo-Egypt. His current research interests are in multimedia processing and cryptography.