Robust Watermarking Framework with DCT Based Encryption

L.Sri Lakshmi
Gudlavalleru Engineering College,
Gudlavalleru.

Mrs. SK. Salma Begum
Gudlavalleru Engineering College,
Gudlavalleru

Abstract **–**

Since several years,, the protection of multimedia data is becoming extremely important. The protection of the multimedia data might be performed with encryption or data hiding algorithms. To address the transmission time, information compression is required. If you take benefit from the character of cryptographic schemes and digital watermarking, the copyright of multimedia contents can possibly be well protected. Our objective will be to give access to the outcomes of one's image integrity and of their origin regardless of the fact that the reputation is stored encrypted. If watermarking and encryption are conducted jointly for the protection stage, watermark extraction and decryption might be applied independently. With the source end original image and watermarked encrypted image is processed. This encrypted watermark image is finally decoded at the receiver end. This proposed work proposes a novel encryption algorithm to encrypt image. The entropy of this very watermarked image and correlation coefficient of extracted watermark image is amazingly not far away from ideal values, proving the correctness of proposed algorithm. In the proposed system, a Watermarking Scheme based on DWT with encryption algorithm, will be developed to improve the robustness and protection along with security. **Also experimental results show resiliency of a given scheme against large blurring attack like mean and Gaussian filtering, linear filtering Thus proving the security, effectiveness and robustness of a given proposed watermarking algorithm.**

Keywords **-Watermark, Encryption, JPEG.**

I. INTRODUCTION

The actual procedure of embedding information into another object/signal might be deemed watermarking. Watermarking is mainly made use of for copy protection and copyright-protection. Historically, watermarking has been used to sensitive' information hidden in a different signal. Watermarking has its own applications in image/video copyright protection. The characteristics regarding a watermarking algorithm are normally connected to the application form finally it was develop for. Some fundamental explain the circumstances of watermarking: i) Imperceptibility - A watermark is termed perceptible if its presence among the marked signal is noticeable, but non-intrusive. A watermark is termed imperceptible if the cover signal and marked signal are indistinguishable with regards to a fantastic perceptual metric. Watermarking is used for embedding invisible or visible information into images whereas encryption is the process of encoding messages or information so that eavesdroppers or hackers cannot read through it, only authorized users can read. There will be applications by which both encryption and watermarking must be done to produce authentication along with to preserve the confidentiality of one's image data. In these cases, however, if encryption and watermarking processes typically are not outside of each other, to authenticate images one will have to decrypt the reputation first then retrieve the added watermark. To put it differently just to authenticate the figures confidential data needs to be disclosed at intermediate nodes during which the comprehensive data transmission happens. Hence the is need for creating an approach wherein both encryption and watermarking can easily be done simultaneously and independently in a way that encryption doesn't prohibit the watermark embedded among the images.

Actually, encrypted data need an additional level of protection in order to keep control on them after the decryption phase. In fact, when the ciphered data is deciphered by the authorized user, it is unprotected and it can be easily modified, tampered, or stolen. The scientific community started focusing on the possibility of providing both security services simultaneously and therefore to have the chance of watermarking encrypted data and detecting the watermark before and after decryption. This allows to work in the encrypted domain, operating on ciphered data without giving access to the plain one and increasing the operation efficiency.

The process of watermarking begins when the encoder inserts watermark into image, producing watermarked image. The decoder extracts and validates the presence of watermarked input or unmarked input [1]. The transform domain watermarking systems are based on Fourier and Cosine transform which are the invertible transform applied to the image where the coefficients are modified by the watermark data. The Discrete Cosine transform watermarking divides the image into different frequency band and choose the middle frequency band for watermarking. The method that we are going to use on

our approach is wavelet watermarking. The Wavelet domain watermarking system is the multi-band watermarking scheme. The attacker may not be able to detect the embedded watermark without knowing the parameter. The original image is decomposed into wavelet coefficients and then multi-energy watermarking scheme based on the qualified significant wavelet tree.

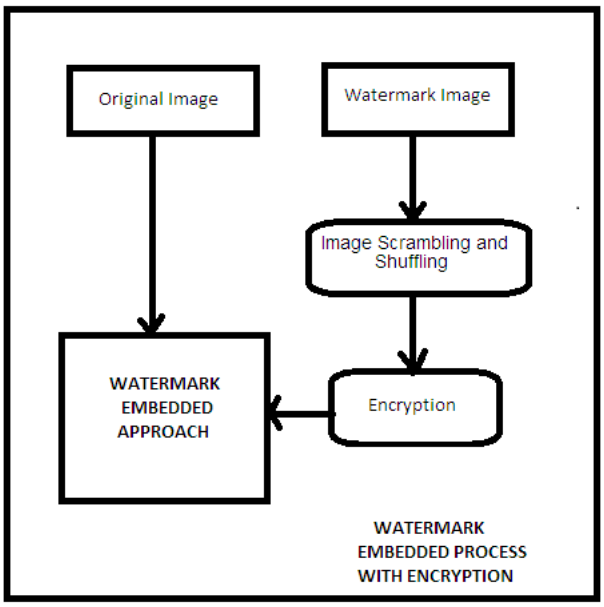
II. LITERATURE SURVEY

A. V. Subramanyam et. al., focussed according to the robust watermarking technique for JPEG2000 images a situation where the watermark can possibly be embedded within a predictable manner in compressed-encrypted bytestream. The approaches near them are classified as the bytestream encryption from the symmetric stream cipher RC4 and after that embed robust watermark over the images in the compressed-encrypted domain [1] and [4]. Possibly one of the other encryption algorithms would be the RC5. RC5 provides more security in comparison to the RC4 encryption algorithm. Omar Elkeelany and Adegoke Olabisi, presented performing at maximum RC5- integrated architecture with variable key registration, enhanced security and improved encryption throughput.

[6] proposed a content-dependent watermarking technique, which embeds the watermark in an encrypted format, but the host signal is still in plain text format. The algorithm may not be directly applied when the content is in encrypted format, in that case the distortion introduced in the host signal may be large.

In [7] Sun et.al. proposed a semi fragile authentication system for JPEG2000 images. However, this scheme is not a fully compressed and encrypted domain watermarking compatible as it derives the content based features for watermarking from the plain text. To our knowledge, the proposed technique is the first work which does fully compressed encrypted domain watermarking. [8] proposed a technique for invisible Digital Watermarking through Encryption where the image is encoded within another image (cover image). Firstly, the cover image and the target image can be adjusted by resize function. Secondly, only the final encrypted image i.e.cover image and target image is sent over the network. This image is finally decoded at the receiver end. Puech and Rodrigues [1] present a method of partial or selective encryption for JPEG images. It is based on encoding of some Huffman bit stream with AES cipher. M.A. Mohamed [9] proposed a hybrid image protection scheme to establish a relation between the data encryption key and the watermark. Prepositioned secret sharing allows the reconstruction of different encryption keys by communicating different activating shares for the same prepositioned information. Each activating share is used by the receivers to generate a fresh content decryption key. In the proposed scheme, the activating share is used to carry copyright or usage rights data. The bit stream that represents this data is also embedded in the content as a visual watermark. When the encryption key needs to change, the data source generates a new activating share, and encrypts the corresponding data with the key constructed from the new activating share. Before transmission, the encrypted data is embedded in a multimedia stream. Each receiver can extract the encrypted data from the host image, and decrypt this data after reconstructing the same key.

III. PROPOSED SYSTEM



Encryption Process:

Step 1: Collect data from the sender: XL: X-Length, YL:Y-Length, r:radius, Pn: Pattern, P-Image Plaintext (stream of bits).

Step 2: Create Cartesian Grid plain (XL*YL) and add 1 bit of data at every integral Cartesian point; in creation of grid verify the following conditions

If P = (XL*YL) then create grid with (XL*YL) points

Else

If P < (XL*YL) then fill the grid points with noise value.

Else

If P > (XL*YL) then reenter the value of XL and YL.

Step 3: Generate random bits at the edge of the grid using BLUM BLUM SHNB GENERATOR

- Based on the squaring one-way function
  - Let p, q be two odd primes and $p \equiv q \equiv 3 \bmod 4$
  - Let n = p*q
  - Let x_0 be a seed which is a quadratic residue modulo n

    $x_i = x_{i-1}^2 \bmod n \qquad i \geq 1$

Output

$(x_1, x_2, \ldots, x_k)$

$y_i = x_i \bmod 2$

$Y = (y_1 y_2 \ldots y_k)$ ⇓ pseudo-random sequence of K bits

Step 4: Generate Circles using *Bresenham's circle algorithm* with centers as shown below

(0, 0), (0, 2r), (0, 4r)…. (0, YL)
(r, r), (r, 3r), (r,5r)…. (r,YL-r)
(2r, 0), (2r, 2r), (2r, 4r)… (2r, YL)
(3r, r),(3r, 3r), (3r,5r)… (3r, YL-r)

Step 5: Rotate each circle by angle θ (θ being randomly generated) for each Θ add it to the key.

Step 5.1*: Shift (0, 0) to center of respective circle*

$$(x', y') = (x + \mathrm{x}, y + \mathrm{y})$$

Step 5.2: Rotate the circle with θ generated randomly which will make the new coordinates

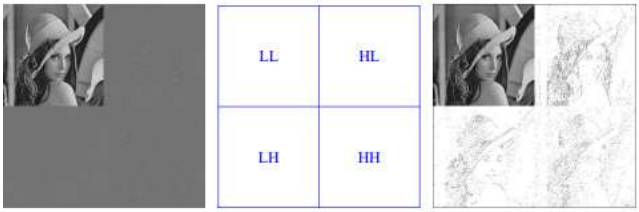
$$(x', y') = ((x\cos\theta - y\sin\theta), (x\sin\theta + y\cos\theta))$$

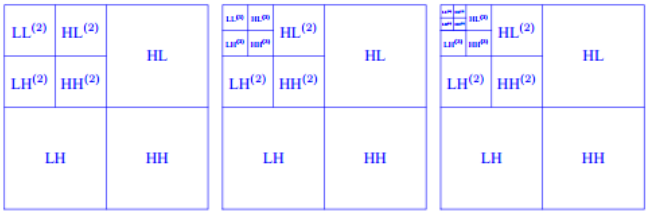
Step 5.3: Shift the origin back to (0,0) using the formula in 5.1

Step 6: *Repeat step 5* for each circle that exists in the grid, follow the pattern that is given by the user.

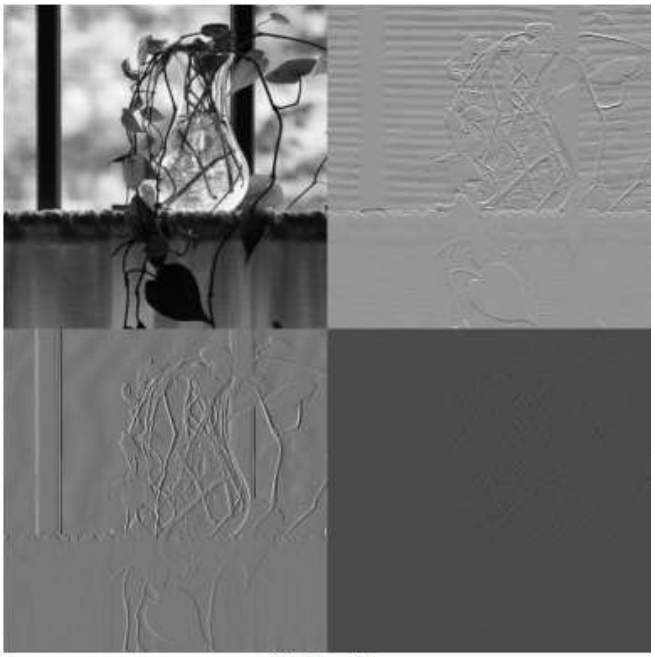
Watermark Embed Process:

LL: The upper left quadrant consists of all coefficients, which were filtered by the analysis low pass filter h˜ along the rows and then filtered along the corresponding columns with the analysis low pass filter h˜ again. This subblock is denoted by LL and represents the approximated version of the original at half the resolution. HL/LH: The lower left and the upper right blocks were filtered along the rows and columns with h˜ and g˜, alternatively. The LH block contains vertical edges, mostly. In contrast, the HL blocks shows horizontal edges very clearly.HH: The lower right quadrant was derived analogously to the upper left quadrant but with the use of the analysis high pass filter g˜ which belongs to the given wavelet. We can interpret this block as the area, where we find edges of the original image in diagonal direction. The two dimensional wavelet transform can be applied to the coarser version at half the resolution, recursively, in order to further décor relate neighboring pixels of the input image.

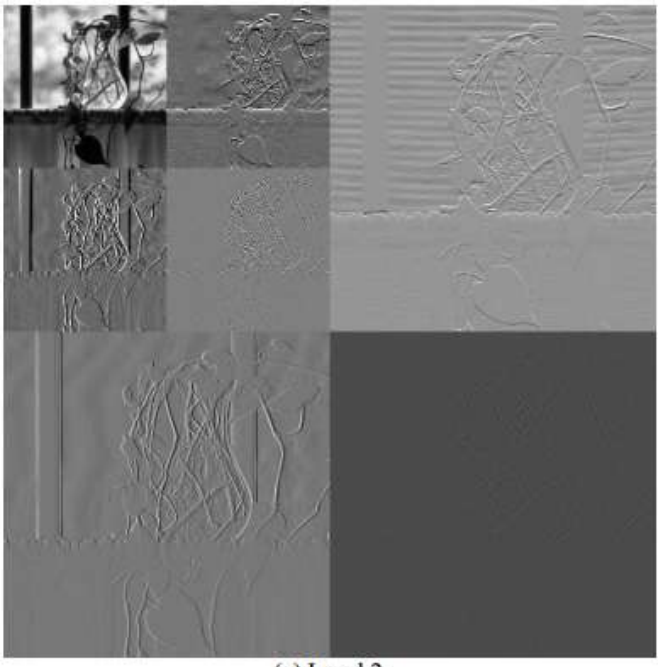




(a) two levels of 2D-DWT (b) three levels of 2D-DWT (c) four levels of 2D-DWT



(b) Level 1

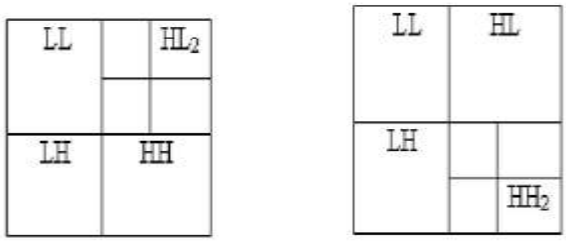


(c) Level 2

Watermark Embedding Procedure:

Step 1. Apply DWT to decompose the cover host image into four non-overlapping multi-resolution subbands: LL1, HL1, LH1, and HH1.

Step 2. Apply DWT to the HL1 sub-band to get four smaller sub-bands, and choose the sub-band HL2 as shown in Figure 1(a). Or, apply DWT to the HH1 subband to get four smaller sub-bands and choose the subband HH2, as shown in Figure 1(b).



(a) (b)

decomposition of the original image.

Step 3. Divide the sub-band HL2 (or HH2) into 4x4 blocks.

Step 4. Apply SVD to each block in HL2 (or HH2) according to Equation 1, where A in the equation refers to any block in the chosen sub-band.

$$A = USV^T \quad (1)$$

Step 5. Re-formulate the grey-scale watermark image into a vector of zeros and ones.

Step 6. Modify the singular values matrix S of each block according to the value of the watermark bit. If the watermark bit is 0, S is modified according to the watermark embedding formula given in Equation 2, where a is a scaling factor that has a value in the range

$1 \geq \alpha \geq 0.$

$$S' = S\ (1 + \alpha) \quad (2)$$

otherwise, if the watermark bit is 1, S remains unchanged as in Equation 3.

S'=S ----------→ (3)

Step 7. Apply inverse SVD (ISVD) to each block A by multiplying the orthogonal matrices U and VT with the modified matrix S', as shown in Equation 4.

$$A = US'V^T \quad (4)$$

Step 8. Apply the inverse DWT (IDWT) on the DWT transformed image, including the modified sub-band, to produce the watermarked cover host image.

Watermark Extraction Procedure:

Step 1. Decompose the watermarked image using DWT into four non-overlapping multi-resolution sub-bands: LL1, HL1, LH1, and HH1. Again we apply DWT to the HL1 sub-band to get sub-band HL2 or to the HH1 sub band to get sub-band HH2, as shown in Figure 1.

Step 2. This algorithms is a non-blind watermarking algorithm, and thus requires the original image in the extraction process. Therefore, we also decompose the original image using DWT into 4 non-overlapping multi-resolution sub-bands: LL1, HL1, LH1, and HH1. Again, we apply DWT to the HL1 to get sub-band HL2 or to the HH1 to get sub-band HH2,, as shown in Figure 1.

Step 3. Divide sub-band HL2 (or HH2) of the original and watermarked images into 4 x 4 blocks.

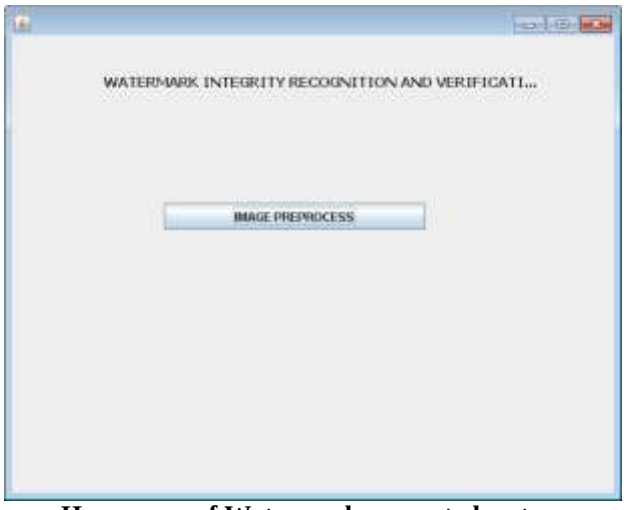
Step 4. Apply singular value decomposition SVD to each block in the chosen subband of the watermarked image and extract the singular values matrix SI using equation 1. Similarly, apply SVD to each block in the sub-band of the original image and extract the singular values matrix S2 using Equation 1.

Step 5. Find the difference between all singular values in SI and S2 If the difference exceeds a threshold value of 0.75, take the extracted watermark bit as bit 0, otherwise, take it as bit 1.

Step 7. Reconstruct the watermark using the extracted watermark bits, and compute the similarity between the original and extracted watermarks.

IV.EXPERIMENTAL RESULTS

All experiments were performed with the configurations Intel(R) Core(TM)2 CPU 2.13GHz, 2 GB RAM, and the operating system platform is Microsoft Windows XP Professional (SP2).



Home page of Watermark encrypted system

Options in the proposed system

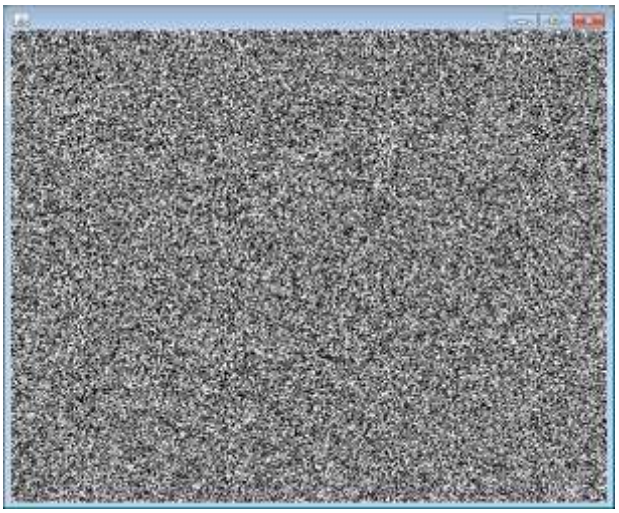
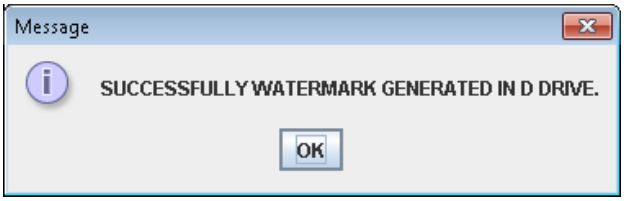


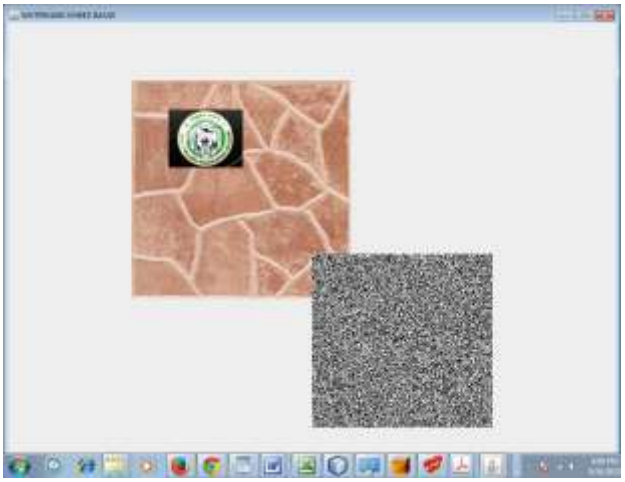
Image in encrypted format

Embedding the logo to the original image

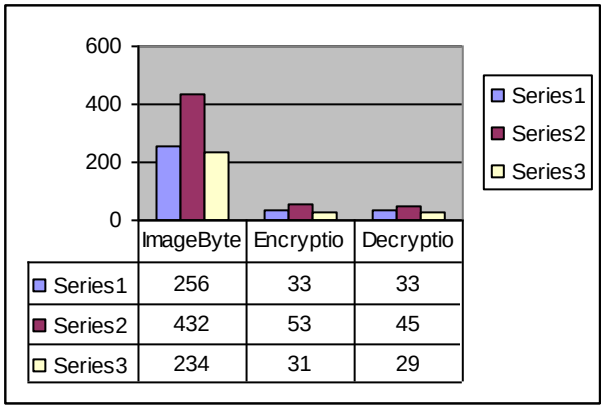
Embedding the encrypted image to original image for more security.

Encryption process is selected



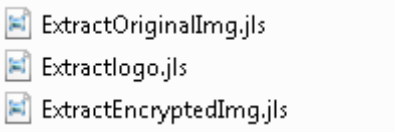


Complete double embedding process image



Graph shows the comparision between Image sizes with the embed and extract times.

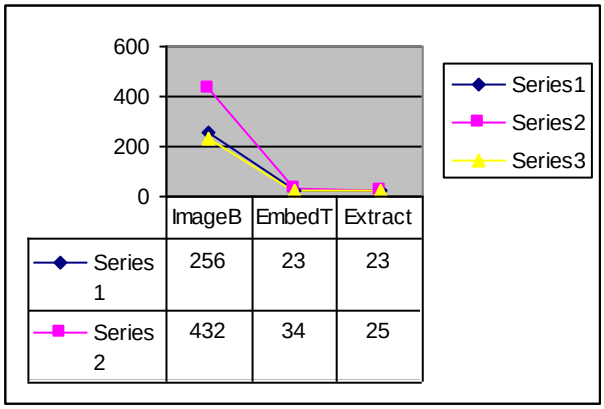
Extraction option is selected.



Files created after extraction.

Performance Analysis:

Graph shows the comparison between Image in bytes with the Encryption decryption time.



V. CONCLUSION AND FUTURE SCOPE

The increasing amount of digital exchangeable data generates new information security needs. Multimedia documents and specifically images are also affected. Users expect that robust solutions will ensure copyright protection and also guarantee the authenticity of multimedia documents. In the current state of research, it is difficult to affirm which watermarking approach seems most suitable to ensure an integrity service adapted to images and more general way to multimedia images. Watermarking Scheme based on DWT with encryption algorithm, will be developed to improve the robustness and protection along with security.

REFERENCES

[1] A. V. Subramanyam, Sabu Emmanuel and Mohan S. Kankanhalli, "Robust Watermarking of Compressed and Encrypted JPEG2000 Images", IEEE Transactions on Multimedia, Vol. 14, no. 3, pp. 703-716, June 2012.

[2] Anjan Pal and Snehasish Banerjee, "Embedment of Encrypted Text and Secret Images for Digital Image Watermarking," World Applied Programming, Vol .1, no. 3, pp. 132-137 ,August 2011.

[3] S. Hwang, K. Yoon, K. Jun, and K. Lee, "Modeling and implementation of digital rights," J. Syst. Softw., vol. 73, no. 3, pp. 533–549, 2004.

[4] A. Subramanyam, S. Emmanuel, and M. Kankanhalli, "Compressed decrypted domain JPEG2000 image watermarking," in Proc. IEEE Int. Conf. Multimedia and Expo, pp. 1315–1320, 2010.

[5] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative Watermarking and encryption for media data," Opt. Eng., vol. 45, pp. 1–3, 2006.

[6] Ricardo L. de Queiroz, " Processing JPEG-Compressed Images and Documents," IEEE Transactions on Image Processing, vol. 7, no. 12, pp. 1661-1672, Dec 1998.

[7] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems," International Journal of Information and Communication Engineering, 3:8, pp. 537-542, 2007.

[8] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh, "Journal of Computing, vol. 3, Issue 4, ISSN 2151-9617, pp. 1-8, , April 2011.