A New Multi Watermarking Algorithm for Medical Images using DWT and Hash Functions

Alavi Kunhu
Electronics Engineering Department
Cochin College of Engineering and Technology
Kerala, India
alavi@cochincet.ac.in

Fatma Taher and Hussain Al-Ahmad
Electrical and Computer Engineering Department
Khalifa University of Science, Technology and Research
Sharjah, UAE
Fatma.taher@kustar.ac.ae, alahmad@kustar.ac.ae

Abstract*—In this paper, we propose a blind digital multi-watermarking algorithm for the copyright protection and authentication of medical images. When medical images are transmitted and stored in hospitals, strict security, confidentiality and integrity are required to protect from the illegal distortion and reproduction of the medical information. Medical image watermarking requires extreme care when embedding watermark information in the medical images because the additional information must not affect the image quality as this may cause the wrong diagnosis. The proposed algorithm contains one robust watermark for the ownership of the image and two fragile watermarks for checking the authenticity. The first two watermarks are embedded in the wavelet domain, while the third watermark is embedded in the spatial domain. In the proposed algorithm, the medical image is divided into two regions, called the Region of Interest and Region of Non Interest and all the three watermarks are embedded in the Region of Non-Interest. The new medical watermarking technique offers high peak signal to noise ratio and similarity structure index measure values. The technique was successfully tested on a variety of medical images and the experimental results show that the robust watermark survived many intentional and non intentional attacks, while the fragile watermark is sensitive to any slight tampering on the medical images.

***Keywords*— Watermarking; Medical Images; ROI; RONI; DWT; Hash functions; PSNR; SSIM**

I. INTRODUCTION

Nowadays, due to the rapid development of information technology and telecommunication, in the medical field, many traditional diagnoses are being replaced by e-diagnosis for effectiveness, convenience and security. Medical images are captured, stored and send to radiologist and doctors via electronic means. These images need to be secured and protected from any image manipulations. Also the image should be associated with a unique information regarding the patient. Usually hospitals either use patient number or the mobile phone of the patient. The mobile phone of the patient, including the international code is unique worldwide. Watermarking can be used for this purpose [1,2]. Medical image watermarking requires extreme care when embedding additional data within the images because the additional information must not affect the image quality as this may cause the wrong diagnosis.

Digital image watermarking techniques are mainly classified into two categories, spatial domain and transform domain techniques. Usually the transform domain watermarking is more robust than the spatial domain techniques. Another classification of watermarking techniques is blind and non-blind methods based on whether the original image is needed in the watermark extraction process or not. The hidden information can be logo, signature, numbers, text or a mobile phone SIM number [3].

Watermarking can be used to protect the ownership of medical images. This can be done by embedding invisible information inside these images. The invisible watermark must be robust against both intentional and non-intentional attacks. Since the medical images contain sensitive information, an additional type of fragile watermarking is required to protect the integrity of the images to make sure that the content of the image has not been tampered with [4].

This paper deals with a new watermarking algorithm which embeds a robust watermark and one fragile hash-key watermark into the region of non-interest (RONI) in the wavelet domain using the discrete wavelet transform and second fragile hash-key watermark into the image RONI in the spatial domain. The paper consists of 5 sections. The embedding algorithms are discussed in section 2, and the extraction algorithms in section 3. Results and analysis are presented in section 4. Finally, section 5 contains the concluding remarks.

II. EMBEDDING ALGORITHM

In the proposed algorithm the host medical image is first divided into two regions, called Region of Interest (ROI) and Region of Non-Interest (RONI). The ROI is an area which contains important pathological features and must be stored without any distortion. If any watermarking is embedded in this region, it might result in a wrong diagnosis. Therefore, the watermark information should be embedded in RONI [4]. In our algorithm RONI is further divided into three areas called area1, area2 and area3 as shown in Fig. 1. Both area1 and area2 are further sub-divided into 8x8 non-overlapping blocks and transformed into the wavelet domain using 2

978-1-4673-8511-4/15 $31.00 ©2015 IEEE

levels 2D DWT 'haar' wavelet as shown in Fig. 2. Then firstly the robust watermark information of patient's mobile number is embedded in the lower frequency approximation component sub-block (LL2) of area1 using scaled Odd/Even embedding technique using equation 1 [5, 6]. Secondly, find the SHA-256 64 hex unique, fragile hash-key1 for ROI and embed in the lower frequency approximation component sub-block (LL2) of area2 [7, 8, 9]. Finally, find the SHA-256 64 hex unique fragile hash-key2 for watermark embedded combined area1 and area2 and embedded into area3 in the spatial domain using LSB insertion method. Fig. 3 shows a block diagram of the multi-watermarking embedding process. The complete embedding algorithm is summarized in Algorithm 1, where fk indicate the host medical image, region of non-interest area called area1 and area2 and *l*(x,y) represent the watermark information.

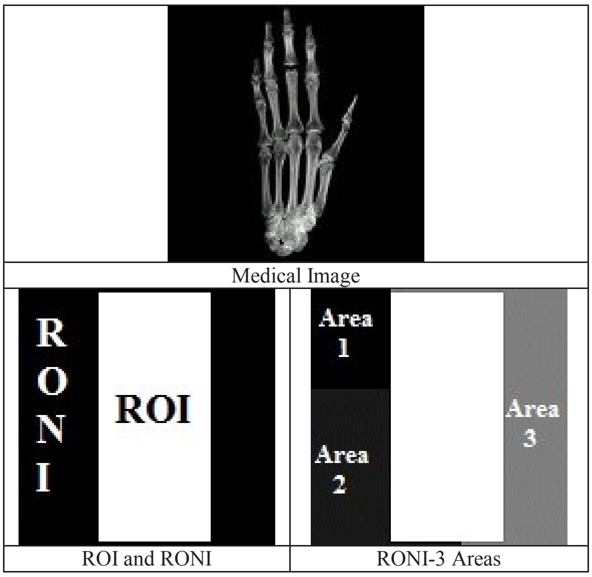

Fig. 1. ROI and RONI division of Medical Image

Algorithm 1: Embedding watermark

Initialize: Wavelet type, Scaling factor (Δ)

Input: Medical image, Watermark information (*lo*)

Output: Watermarked Medical image (fw_k)

- Divide medical image into two regions called
  Region of Interest (ROI) and Region of Non-Interest (RONI)
- Divide RONI into three regions called area1, area2 and area3.
- Divide area1 and area2 into N_{HB} 8×8 sub-blocks and Finding 2-level DWT

  $[LL_1, LH_1, HL_1, HH_1] = DWT[f_k]$

  $[LL_2, LH_2, HL_2, HH_2] = DWT[LL_1]$

- Robust watermark information of patients is embedded in the sub-block (LL2) of area1
- Fragile hash-key1 information is embedded in the sub-block (LL2) of area2
- Fragile hash-key2 information is embedded in area3 in the spatial domain

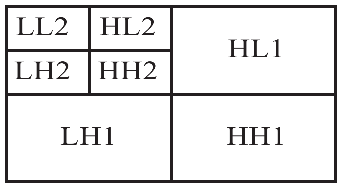

Fig. 2. 2 Levels DWT pyramidal structures

$$[LL, LH, HL, HH] = DWT\{ f_k \} \quad (1)$$

$$if \;\; w = 1 \; then \;\; LL = \begin{cases} \Delta Q_o\left(\frac{LL)}{\Delta}\right) \\ LL \end{cases}$$

$$if \;\; w = 0 \; then \;\; LL = \begin{cases} \Delta Q_e\left(\frac{LL)}{\Delta}\right) \\ LL \end{cases}$$

Where f_k represents the 8x8 sub-block of area1 and area2 of RONI, LL, LH, HL and HH represent the low frequency and high frequency components of the discrete wavelet transform. w represents the watermark information, Q_e indicates even quantization while Q_o indicates odd quantization to the nearest integer number. The Δ is the quantization scaling factor.

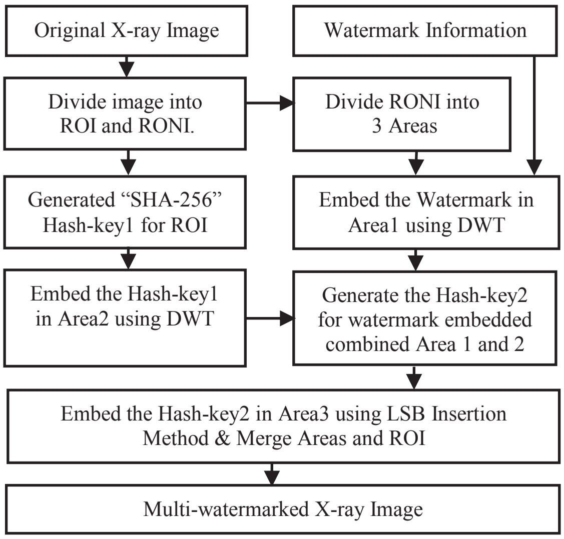

Fig. 3. Multi-watermark embedding process

III. EXTRACTION OF WATERMARKS

A. *Robust Watermark Extraction Algorithm*

Initially we need to extract the robust watermark for identifying the owner of the medical image. This is done by finding the 2 level discrete wavelet transform decomposition of area1 in RONI of the multi watermarked medical image using 'haar' wavelet. Then robust watermark information is extracted from the low frequency block components by using the scaled odd/even extraction algorithm of equation 2 [10, 11]. A block diagram illustrating the robust watermark decoding process is as shown in Fig. 4.

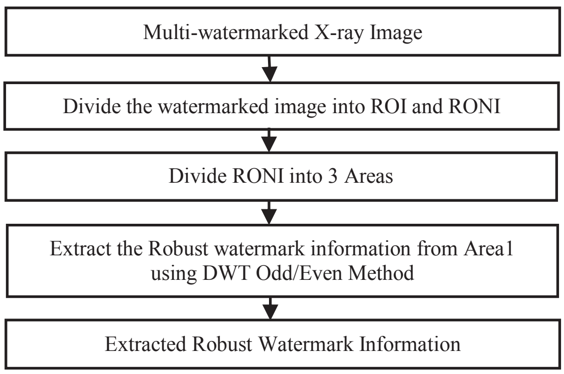

Fig. 4. Robust watermark decoding process

B. *Fragile Hash-key1 Watermark Extraction Algorithm*

SHA-256 fragile hash-key1 is used to check the authenticity of ROI for medical images. The fragile decoding algorithm first divides the watermarked image into ROI and RONI. RONI is further divided into three areas and then extracts the watermarked hash-key1 information from the lower frequency approximation component sub-block (LL2) of the area2 and compares it with the re-generated hash-key from ROI. If they match, then it means RONI is authentic, else it is not authentic. A block diagram illustrating the fragile hash-key1 decoding process is as shown in Fig. 5.

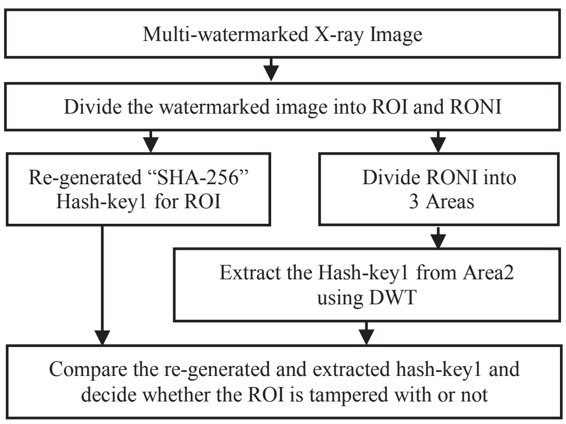

Fig. 5. ROI fragile hash-key1 decoding process

The robust watermark and fragile hash-key1 watermark are extracted using the following equation:

$$Q\left(\frac{LL2}{\Delta}\right) \qquad (2)$$

$$\rightarrow if \;\; odd, then \;\; w(i) = 1$$

$$\rightarrow if \;\; even, then \;\; w(i) = 0$$

Where Q points to the nearest quantization value and Δ is the scaling factor.

C. *Fragile Hash-key2 Watermark Extraction Algorithm*

SHA-256 fragile hash-key2 is used to check the authenticity of RONI for medical images. A block diagram illustrating the fragile hash-key2 decoding process is as shown in Fig. 6

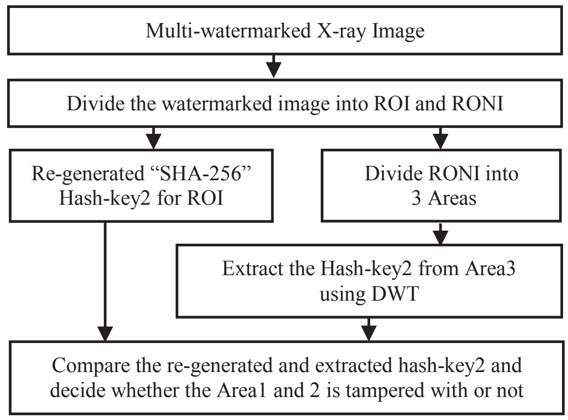

Fig. 6. Area1 and 2 fragile hash-key2 decoding process

IV. RESULTS

The proposed multi-watermarking algorithm is tested on various medical X-ray images. Examples are shown in Fig. 7 where each X-ray image is 512x512 pixels and the robust watermark information is the personal mobile number. The DWT scaling factors used are 8, 16 and 24. 'SHA256' hash functions were used to generate a unique fragile hash-key1 and hash-key2.

The distortion caused to the medical X-ray images were assessed by using the peak signal-to-noise ratio (PSNR) and the structural similarity index measurement (SSIM) [6, 7]. The peak signal to noise ratio (PSNR) is used as a metric to measure the quality of the watermarked host medical images. The PSNR penalizes the visibility of noise in the host image. Thus, two medical images that are exactly the same will produce an infinite PSNR value. PSNR is given by.

$$PSNR = 10.log_{10}\left(\frac{255^2}{MSE}\right) \qquad (3)$$

The SSIM is a measure that compares local patterns of pixel intensities that have been normalized for luminance and contrast. The higher SSIM is the larger the similarity between the compared images. SSIM is given by:

$$SSIM(fo,fw) = (L(fo,fw))^{\alpha}.(C(fo,fw))^{\beta}.(S(fo,fw))^{\gamma}$$

$$L(o,w)=\frac{2\mu_X\mu_Y+A}{\mu_X^2+\mu_Y^2+A}, \quad C(o,w)=\frac{2\sigma_X\sigma_Y+B}{\sigma_X^2+\sigma_Y^2+B}, \quad (4)$$

$$S(o,w)=\frac{\sigma_{XY}+C}{\sigma_X\sigma_Y+C}$$

Where *fo* represents the original medical image and *fw* represents a watermarked medical image. *L, C* and *S* represent the luminance, contrast and structure components respectively, while *α, β, γ* are parameters used to adjust the relative importance of the luminance, contrast and structure components.

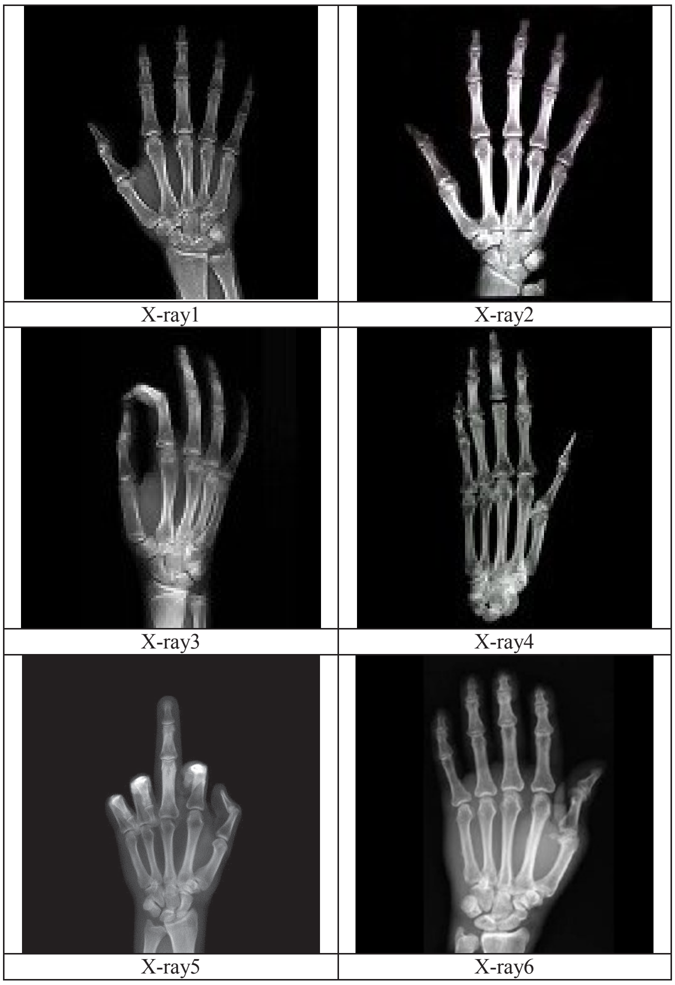

Fig. 7. X-ray images

The performance analysis of medical images is shown in Tables 1 and 2. From Table 1 and Table 2, it should be noted that as the DWT scaling value increases, then the PSNR and SSIM starts to decrease. In our analysis the PSNRs of the multi-watermarked images were greater than 46dB, while the SSIM were larger than 0.95 and the watermark information were invisible. Fig. 8 shows the PSNR analysis of watermarked medical images and Fig 9 shows the SSIM performance analysis.

TABLE 1. PSNR ANALYSIS OF WATERMARKED X-RAY IMAGES

Image	Δ=8	Δ=16	Δ=24
X-ray1	58.6570	52.6728	49.1620
X-ray2	57.4108	51.7230	48.0223
X-ray3	53.1288	50.2271	47.6470
X-ray4	55.4152	49.5478	46.0327
X-ray5	56.6670	50.6628	47.1120
X-ray6	55.4100	50.7233	47.0222

TABLE 2. SSIM ANALYSIS OF WATERMARKED X-RAY IMAGES

Image	Δ=8	Δ=16	Δ=24
X-ray1	0.9955	0.9861	0.9765
X-ray2	0.9944	0.9831	0.9712
X-ray3	0.9907	0.9868	0.9788
X-ray4	0.9902	0.9710	0.9511
X-ray5	0.9935	0.9841	0.9745
X-ray6	0.9924	0.9811	0.9701

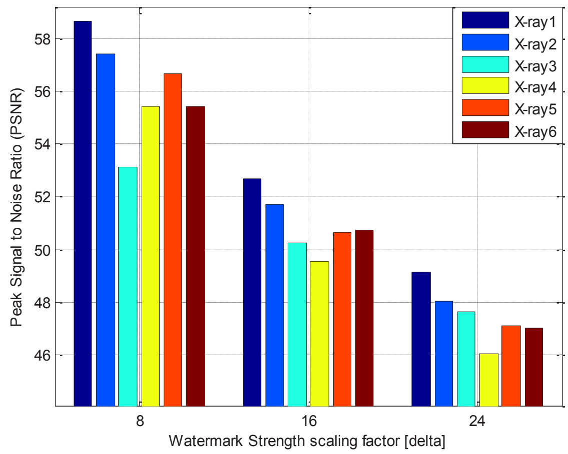

Fig. 8. PSNR analysis of watermark medical images

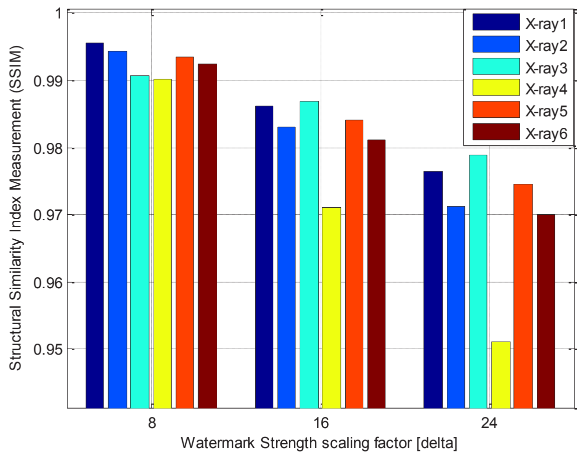

Fig. 9. SSIM analysis of watermark medical images

In the new algorithm, the SHA256 generates 64 hex length hash-keys. Table 3 shows the SHA256, fragile hash-key1 generated for ROI and hash-key2 for RONI of medical image X-ray1. Any modification even if a single pixel value is increased or decreased by1 at any location in the ROI block of the watermarked medical image will make a difference between the regenerated hash-key1 and the recovered hash-key1. While modification in the RONI block will make a difference between the regenerated hash-key2 and the recovered hash-key2. Table 4 shows the details about tampering detection of watermarked medical image based on fragile hash-keys comparisons. This proves that the new proposed hash algorithm is very sensitive to any modifications or tampering.

TABLE 3. SHA-256 FRAGILE HASH-KEY1 AND HASH-KEY2

Hash-key1 (64 hex length)	8e4c38253688cd1b88836f0f11fd8089 9825618b1e8969117107451ee48808dd
Hash-key2 (64 hex length)	21426167e070bd84e5d564f35d356f6e 77cd568dba2de62d40ab9048b8c947f0

TABLE 4. FRAGILE WATERMARK PERFORMANCE ANALYSIS UNDER TAMPERING ATTACKS FOR X-RAY1 IMAGE

Extracted and Regenerated		**Conclusion**
Hash-key1	**Hash-key2**	
same	same	No Tampering
different	same	Tampering on ROI
Same	different	Tampering on RONI
different	different	Tampering on ROI & RONI

The robustness of the algorithm are checked by applying various attacks such as JPEG compression, image scaling and image rotation. Table 5 demonstrates the limits of the recovery performance of the robust watermark information under various scaling values.

TABLE 5. ROBUST WATERMARK PERFORMANCE ANALYSIS UNDER VARIOUS ATTACKS FOR X-RAY1 IMAGE

Δ	JPEG Attack	Resize Attack	Rotation Attack
8	upto 75%	upto 35%	2.5degree
16	upto 35%	upto 35%	2.5degree
24	upto 30%	upto 35%	2.5degree

V. CONCLUSION

This paper has presented a new blind multi watermarking technique, which embeds one robust watermark information and two fragile watermarking information for the protection and authentication of medical images using DWT-Hash. Medical image protection and authentication are very important in any e-health environment. The proposed algorithm has been successfully tested on a number of medical images. The Hash based fragile authentication watermark information are very sensitive to any small modification to the medical images, while the DWT based ownership watermark information is robust against several attacks such as JPEG, scaling and rotation attacks.

REFERENCES

[1] X. Luo, Q.Cheng and J. Tan, "A Lossless data embedding scheme for medical images in application of e-diagnosis," In proceeding of the 25th Annual International Conference of the IEEE EMBS, Mexico, September, 2003, pp.852-855.

[2] C.Woo, J. Du and B.Chen," Multiple watermark method for privacy control and tamper detection in medical images," In proceeding of APRS Workshop on Digital Image Computing (WDIC), Australia, 2005, pp. 59-64.

[3] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, "A New Blind Image Watermarking of Handwritten Signatures Using Low-Frequency Band DCT Coefficients," In proceeding of ICSPC, the IEEE International Conference on Signal Processing and Communications Dubai, United Arab Emirates, 2007, pp. 1367-1370.

[4] G. Coatrieux and L. Lecornu,"A Review of Image Watermarking Applications in Healthcare," In proceeding of 28th Annual International Conference of the IEEE: Engineering in Medicine and Biology Society, EMBS '06. 2006, pp. 4691-4694.

[5] S. Al-Mansoori and A. Kunhu, "Robust Watermarking Technique based on DCT to Protect the Ownership of DubaiSat-1 Image against Attacks", In proceeding of IJCSNS International Journal of Computer Science and Network Security, June 2012, Vol.12, No.6, pp.1-9.

[6] Saeed AL-Mansoori and Alavi Kunhu, "Multi-Watermarking Scheme for Copyright Protection and Content Authentication of DubaiSat-1 Satellite Imagery", In proceeding of SPIE of Optics and Photonics Conference 2013, Vol.8871, California, USA, September 2013.

[7] Alavi Kunhu and Hussain Al-Ahmad, "A New Watermarking Algorithm for Color Satellite Images Using Color Logos and Hash Functions", 5th IEEE International Conference on Computational Intelligence, Communication System and Networks - CICSYN2013, Madrid, Spain, June, 2013, pp.251-255.

[8] Z. Zhang, H. Peng and X. Long, "A Fragile Watermarking Scheme Based On Hash Function for Web Pages", International Conference on Network Computing and Information Security, May 2011, pp. 417-420.

[9] Huang Daren, Liu Jiufen, Huang Jiwu and Liu Hongmei "A DWT based image watermarking algorithm", ICME IEEE International Conference on Multimedia and Expo, August 2001, pp. 313-316.

[10] A. Al-Gindy, H. Al-Ahmad, R. Qahwaj, and A. Tawfik, "A frequency domain adaptive watermarking algorithm for still colour images," in International Conference on Advances in Computational Tools for Engineering Applications, ACTEA '09. , Beirut, Lebanon, July 2009, pp. 186-191.

[11] A. Al-Gindy, H. Al-Ahmad, R. Qahwaj, and A. Tawfik, "A new watermarking scheme for colour images captured by mobile phone cameras" IJCSNS International Journal of Computer Science and Network Security, July 2009, vol. 9, pp. 248-254.