International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 315-328
http://dx.doi.org/10.14257/ijsia.2015.9.6.29

A Novel Authentication Scheme for Lossy Compressed Images

Mona A. M. Fouad[1] and Ahmed Mokhtar A. Mansour[2]

[1]Computers & Systems Department
National Telecommunication Institute, Cairo, Egypt
[2]Nile Innovations, Cairo Egypt
[1]mfouad@nti.sci.eg, [2]ahmedmokhtar_adu@yahoo.com

Abstract

In this paper, a novel scheme is proposed for watermarking lossy compressed images just before transmission and authenticating them once they are received, away from the core of the compression and de-compression processes. The scheme is inserted into the Joint Photographic Expert Group (JPEG) structure that is encoded using the Discrete Cosine Transform (DCT) at specified locations. The watermark information is extracted from and embedded into specified DCT coefficients, following novel criteria. The scheme is robust to lossy compression; though it is fragile, exposing any slight changes of the probe images. The scheme is also blind, needs no prior information about the original image or the watermark information to authenticate the received image. Experimentally, if the received watermarked data is not manipulated, the proposed scheme verifies them as 'authenticated'. On the other side, if geometrical or image processing attacks are applied to the watermarked images, they are then verified successfully as 'not authenticated'. The proposed scheme is further evaluated and compared to similar authentication schemes. The noise added to the original image due to embedding the watermark information is 0.063 dB (decibel), overcoming all results in the reviewed literature.

Keywords: *Authentication, Blind, DCT, Fragile, JPEG, Robust, Security, Watermarking*

1. Introduction

Authentication is a must if images are transmitted using public networks. This is to make sure that the received image is the transmitted one and any malicious attack is discovered. Digital signature and watermarking are two well known approaches to stamp the transmitted image and to verify the received image. Two parameters should be considered for authenticating images, the image type and the application. Image types consider compressed or uncompressed, color/ gray or black/white images. Online, offline, medicine and military applications are considered for application based authentication schemes.

The proposed scheme authenticates the lossy compressed JPEG images that encoded based on DCT transform. The scheme is blind and fragile, detecting any slight changes in the compressed image, without needs for any prior information about the original image or the watermark information to authenticate the received image. The watermark information is embedded into the three LSBs (Least Significant Bits) of certain elements of specified quantized matrices. This is why the noise due to embedding the watermark information is negligible, corresponding to 0.063 dB as average distortion for the whole image. The proposed scheme is applicable for online applications and it is suitable for the medical and confidential images.

The literature is reviewed extensively in Section II, focusing on authentication for compressed images. The proposed scheme is explained in details in section III. Section IV

ISSN: 1738-9976 IJSIA

includes experimental results and evaluation of the developed authentication scheme. The complete work is concluded in section V, with directions to the future work.

2. Authenticating Lossy Compressed Images

By reviewing the literature, the watermarking based image authentication schemes that handle lossy compressed images could be categorized into two parties. The first party emulates data loss due to image transformation and quantization process [1-3], while the other party embeds watermarking information into the transformed coefficients. The wavelet transformation based semi-fragile authentication schemes are proposed in [4-13] and a fragile scheme is developed in [14] and [15]. The cosine transformation space is considered in [16-18] for proposing watermarking/authentication schemes. The authentication scheme composing both DWT and DCT is proposed in [19]. A special technique based on block truncation code is proposed in [20], while a sparse coding based authentication scheme is proposed in [21].

A backward-compatible image authentication based on distributed source coding is demonstrated in [1]. The user receives the image to-be-authenticated as the output of a two-state lossy channel that models legitimate and illegitimate modifications. The authentication data consist of a Slepian-Wolf encoded quantized image projection of the source image and a digital signature of that version. The verification decodes the authentication data with the help of an authentic image. The size of the authentication data is the performance key to distinguish between legitimate encoding variations of the image and illegitimate modifications. The Slepian-Wolf bit-stream size should be less than 66 bytes or 2.3% of the encoded file sizes for 30 dB as reconstructed image quality.

An approximation of the luminance image is embedded into the color components in [2], providing blind and semi-fragile watermarking scheme. A certain key is used to map the position of the specified luminance information taken to the embedded watermarking positions in the colored image. The luminance of the received image is approximated and compared to the watermark information of the corresponding pixels in the colored image using the secrete key. If altered pixels are detected, their colored values are approximated from their corresponding luminance values. Altered pixels are recovered if they represent 50% or less. The PSNR achieved for the watermarked image is less than 37 dB.

In [3], an authentication scheme based on a weighting function exploited that important content information is not uniformly distributed across the image and that illegal operations are usually localized while permissible operations are global in nature. The weighting function is constructed from the extracted feature points. The original image data are then lossy compressed under a weighted norm determined by the weighting function. The highly compressed data together with the description of the weighting function forms the signature that is then being further encrypted and applied as mask to the quantized wavelet coefficients. Checking the authenticity involves computing the distortion between the compressed descriptions of the original image with the current image under the weighted norm. Global distortions are examined by applying Gaussian noise, low-pass filter, and JPEG compression. The image is authenticated successfully, as long as the distortion does not exceed 13 dB.

The authentication scheme in [4] extracted content-based image features, specifically edge information, from the approximation sub-band in the wavelet domain to generate two complementary watermarks. Three-level Haar wavelets transform is applied to the original image, and then Sobel edge detector is applied on the approximation sub-band to generate the first binary watermark sequence. The second binary watermark sequence is generated by concatenating the block pair-based watermark sequence that records the invariant relationship between quantized wavelet coefficients at 64 corresponding positions of each block pair. Both watermarks are embedded into the high frequency

wavelet domain to ensure the watermark invisibility. Only five images were examined achieving PSNR of 39.6 dB in average.

In [5], the image is DWT-transformed with the bi-orthogonal 9/7 wavelet filter, at first, and approximated by four bit planes. Therefore, every wavelet coefficient of the transformed image is quantized to an invariant value. The other coefficients of the dead-zone are left unchanged. Then, all coefficients are hashed using the hashing algorithms; SHA-1 of 160 bits per level, and 728 bit RSA-encryption. Date and time of the captured image are also included in the data to be encrypted. The quantization dither modulation technique is used to embed the encrypted signature as a watermark to the elements of a set of two different quantizers, affecting only one single bit-plane of the quantizers. At the verification site, error correction coding is used to reconstruct the submitted watermark bits of the distorted image. For further noise reduction, the verification algorithm moves the quantized coefficients back to the centre of the hash intervals after the signature bits are extracted to remove the watermark bits and improve image visualization.

In [6], a meaningful binary image watermark is embedded into the least five bits of the lowest sub-bands coefficients of the 3ed bit-plane of the DWT of the input image. The difference of IWT coefficients before and after embedding varies from -15 to +16, achieving PSNR of 42.2 dB in average for the examined two watermarked images.

A stream cipher watermark is embedded into the encrypted JPEG2000 images in [10]. The watermark is inserted into the least significant bit planes of middle resolutions. Maximum number of embedded watermark bits is 9767 adding average noise of 12 dB.

In [14], a scalable fragile authentication scheme is proposed for authenticating scalable JPEG2000 images. Features are extracted from the lowest and highest layers and embedded into the LSBs of selected wavelet coefficients, of the corresponding layers, directly after the quantization step. The set of selected coefficients contains all coefficients with magnitudes greater than or equal to certain threshold that is not completely lost due to scaling. The watermark of the received image is extracted and then compared to the original watermark. If the extracted and the original watermarks are matched, then the image is authenticated.

In [7-9], the watermark is implemented into the DWT domain and is later coupled within the Set Partitioning In Hierarchical Tree (SPIHT) compression algorithm developed in [22], considering image transmission over low-bandwidth and lossy networks. The wavelet based watermarking scheme proposed in [7] transform the original image into the wavelet domain. Then, the lowest band of wavelet coefficients constituting a rough image is scaled to a size determined by the number of watermark bits that fit into that band. Next, an edge map of the scaled, rough image is computed, encrypted, and then inserted into the lowest band of the wavelet coefficients. The watermarked matrix of coefficients is then encoded using network-conscious SPIHT algorithm and then transmitted. In [8] and [9], the watermark is "non-fragile," tolerating distortions due to compression. The watermark is encoded based on the rank-order relationship in local areas throughout the lowest level of the DWT, providing a binary set. The wavelet decomposition coefficients are modified according to this binary sequence. The signature is also embedded and tested within the SPIHT compression algorithm. A signature is a set of bit-string in [9], while it is a set of bits representing the edge maps of the image in [8].

Watermark information is embedded into the least significant bits of specified wavelet coefficients with large magnitudes in [11] and into the middle frequency bands of the DCT coefficients in [16], without corrupting minutiae, to authenticate fingerprint images. The effect of the watermarks on the fingerprint features are measured based on the comparison between the total numbers of extracted minutiae points before and after the embedding process.

Medical images have been considered in [12-15]. In [12], an image is divided into two parts, the region of interest (ROI) and the region of non-interest (RONI). Patient's data are embedded into ROI using a reversible technique, while tamper detection and recovery

data are embedded into RONI. Patient's data and an encrypted message of ROI, is embedded into blocks belonging to ROI providing an embedding map that is combined with recovery information to form the second watermark. The second watermark is then embedded into blocks belong to RONI. In [13], the watermark is embedded into RONI allowing verification of the legitimate changes at the receiving end without affecting ROI. Both works in [12] and [13] embed the watermarks into the decomposed levels of the DWT sub-bands achieving high PSNR except that the segmentation algorithm play a very important role to distinguish between ROI and RONI. An invertible fragile watermarking method is proposed in [15], embedding 10 bytes size of image header into the last 80 bits of the LSB plane of the image.

In [17], an invertible semi-fragile image authentication scheme is proposed. The original image is divided into non-overlapping 8x8 blocks, applying DCT to each block embedding two watermark sets. The first set of watermarks is embedded by modifying six DCT coefficients that are randomly selected from the low frequency band of each block using a secret key. Each of the non-overlapped 8x8 blocks is further divided into four non-overlapping 4x4 sub-blocks to estimate four mean pixel values of each sub-block that is used as the second set of watermarks. The watermarks are then embedded into their corresponding 8x8 blocks by replacing the DCT coefficients that is randomly selected from the low-mid frequency band of each block by using a certain key. The received image is divided into non-overlapping 8x8-pixels blocks; DCT is then applied to each block. According to the watermark locations that are determined through the key, six watermarks of each block for authentication are first extracted. The retrieved watermarks of each block are then compared with the original watermarks (generated from the key) to authenticate the block. The block is considered to be tampered if the total number of detected watermarks is greater than a pre-determined threshold. Once the tampered block has been identified, the restoration process is initialized, and then the second set of watermarks is extracted and de-normalized for recovering the tampered blocks by using a secret key. Four extracted watermarks of each block are then restored into one DC and three AC coefficients, concerning that the rest of the AC coefficients are zeros. The average PSNR achieved is 37.61 dB for the authenticated image and 24.71 dB for the restored image.

Work in [18] proposed a watermarking algorithm based on correlation to authenticate image content. The luminance component of the YIQ transformed image is subdivided into 8× 8 non-overlapping blocks. The DCT transform is executed on each block. The watermark sequence is generated from the low frequency coefficients and then is hidden into the middle frequency DCT coefficients of another pseudo-randomly selected block with different embedding strength according to the pre-calculated correlation. The content authentication is implemented through correlation calculation between the low frequency coefficients and the corresponding middle frequency coefficients. The PSNR achieved for the JPEG pepper image is 32.29dB.

Blind Discrete Wavelets Transform—Discrete Fourier Transform (DWT-DFT) composite image watermarking algorithm is proposed in [19]. The algorithm is robust against both affine transformation and JPEG compression. A spread-spectrum-based informative watermark, with a training sequence, is embedded into the coefficients of the lowest sub-band in the DWT domain while a template is embedded into the middle frequency components in the DFT domain to deal with affine transformation. In watermark extraction, the template in a corrupted watermarked image is detected to obtain the parameters of affine transform and convert the image back into its original shape. Then, translation registration is obtained by using the training sequence embedded in the DWT domain and finally the informative watermark is extracted. The PSNR of the original image is reduced by 0.2 dB due to the embedded template.

A Block Truncation Coding (BTC) based authentication scheme is proposed in [20]. A random authentication code is generated for each BTC block and embedded into the

difference value between the quantization levels of each block, achieving PSNR of 40.6 dB in average for the whole image. The difference between two quantization levels of the received block is first computed and then the extracted authentication code is estimated. If the extracted authentication code equals the authentication code, then the bock is classified as authenticated, otherwise it is tampered.

A sparse coding learning is proposed in [21] to extract the intrinsic structure of natural images, adopting Independent Component Analysis (ICA) to yield the sparse representation of natural images. Sixty four-basis functions are learned from 50,000 8x8 gray image patches randomly extracted from natural images. Feature extraction of sparse coding is performed both at sender side and receiver side. The luminance image is extracted from the input compressed color image first and then resized to 64x64. The resized image is subdivided into 64 8x8 blocks and indexed to extract 64 sparse coding coefficients, providing a 4096 feature vector of sparse coding coefficients. The feature vector is then quantized. Accordingly, the Hamming distance between quantized features extracted from two blocks at the same location of two images is computed for measuring similarity between the two corresponding blocks. Two blocks are considered similar if half of the feature vectors are identical, and hence the overall image.

A comprehensive survey for image authentication schemes is presented in [23]. The methods are classified according to the service they provide, that is strict or selective authentication, tamper detection, localization and reconstruction capabilities and robustness against different desired image processing operations. The analyzed image authentication methods are specific to the application (industry, medicine, military, copyright...). For applications where strict integrity is needed, such as medical, military or document images, algorithms that do not tolerate any modification to the image such as strict authentication are very satisfactory. Practically, most applications need to tolerate some content preserving manipulations such as compression, filtering, brightness correction and geometrical transformations. Therefore, the image authentications that are robust against content, preserving manipulations rather than detection of manipulations that change the image content are still needed. In consequence, it is recommended that characteristics would compromise several transformation coefficients to provide robustness against compression and filtering.

Signature based methods are robust, simple, and fully automated but they are not secured enough. Whether they are transmitted separated from the image, or concatenated with it, the image could be ‘not verified’ although it is the original. This is happen when the signature is tampered while the image is not. In addition for being able to be tampered easily when the signature is decrypted.

Watermarking methods based on DWT and/or DCT that emulates data loss due to rounding of the quantized transformed image is unstable due to usage of predefined thresholds. The reviewed DWT or DCT based semi-fragile authentication schemes that embed the watermark into the transformed coefficients may affect the image quality dramatically.

By reviewing the literature it is seen that the authentication for compressed images are still under research consideration. The objective is to embed a watermark that is hard to be detected, while preserving high PSNR, and on the other side it should be tolerant to lossy compression as well as filtering, brightness correction and geometrical transformations. Another main objective is to develop the authentication scheme that is fully automatic without any prior information.

The presented work proposed a watermarking scheme for authenticating JPEG images. The scheme is blind, fragile, automatic, and robust to lossy compression. The proposed watermark is invisible, achieving very high PSNR

3. The Proposed Scheme

The proposed image authentication scheme is included into the JPEG structure, at which the authentication processes are away from the core of the compression and decompression processes.

The JPEG structure is composed of an encoder, at the sender side, and a decoder, at the receiver side [25]. The encoder is composed of color converter, DCT transformer, Quantizer, and Entropy encoder. The color converter transforms the RGB model into YIQ or YUV that identifies a luminance component (Y) separately from the color components (IQ or UV). Before encoding the image, it is subdivided into 8x8 non-overlapped blocks. The DCT transformer performs the Discrete Cosine Transform to each of the 8x8 blocks to discard few high-frequency components. The transformed matrix is then quantized and rounded for digital transmission. At this step the image data lost only little invisible information. The last coding step converts the quantized DCT coefficients into binary form using lossless entropy encoding. The decoder performs the opposite of the encoder, the received entropy encoded data is decoded, de-quantized, and then the Inverse Discrete Cosine Transform (IDCT) is applied. The image is reconstructed by finally converting the YIQ or YUV back into the RGB color model.

The proposed image authentication scheme is composed of two stages. The first stage watermarks the original image before transmission. The second stage authenticates the received image just after receiving the encoded data. A simple block diagrams are presented in Figure 1 and Figure 2, showing the JPEG encoder, and decoder, respectively, exposing the location of the proposed watermarking and authentication processes to be applied.

The watermark is extracted from, and applied to the quantized DCT coefficients after rounding process. Once the encoded watermarked data is received, the authentication stage is applied before decoding. The complete proposed authentication scheme is explained in the next sub-sections.

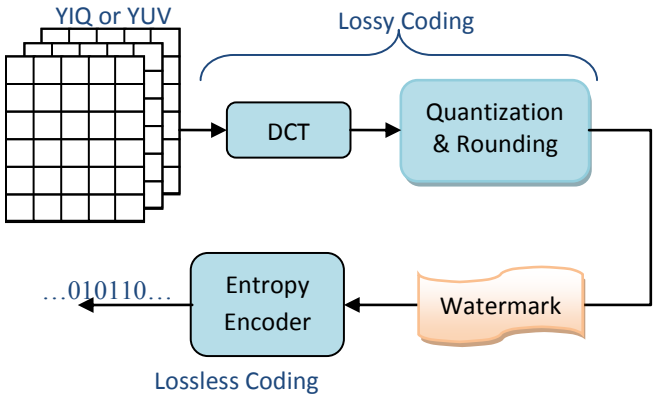

Figure 1. The Proposed Watermarking Block Diagram Embedded into the JPEG Encoder

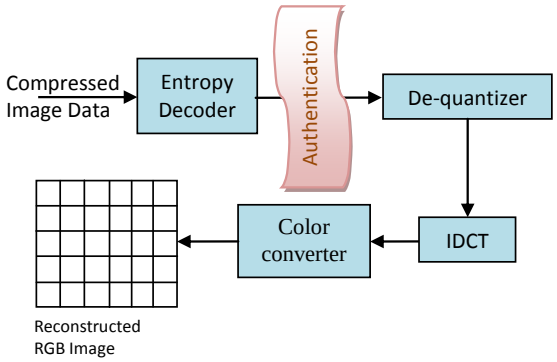

Figure 2. The Proposed Authentication Block Diagram Embedded into the JPEG Decoder

3.1. The Propose Scheme: Watermarking

The watermarking is performed just after the DCT transformed coefficients are quantized and rounded, as seen in Figure 1. The watermark information is extracted from, and embedded into the rounded quantized DCT matrix. In this work, the watermark is histogram based, although it could be any other content information or even hybrid of content and user information. The histogram of the DCT coefficients is estimated, redundancy is eliminated, and the resulted array is then hashed by (1).

$$S(i) = rem(H(i),(N-1)), \quad \forall i \tag{1}$$

Where 'S' is the watermark vector, 'rem' is the remainder, and 'i' is the ith element of histogram vector 'H' of length 'N'.

In details, and as seen in Figure 3, the watermarking process begins by shrinking the rounded quantized DCT matrix, extracts the watermark information, and then embeds the watermark information into the specified coefficients of that matrix. After that the watermarked matrix is enlarged to its original size and the entropy coding is then applied.

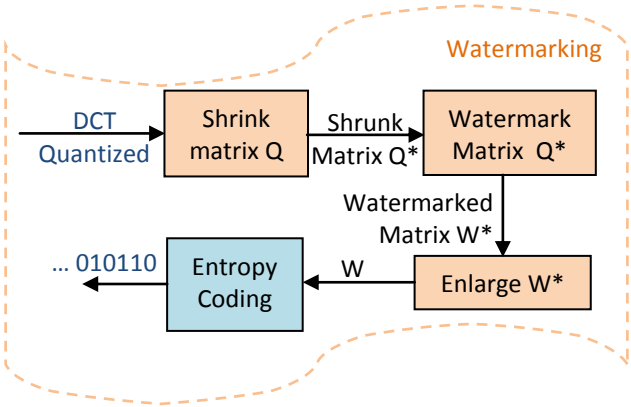

Figure 3. Block Diagram of the Proposed Watermarking

Practically, the following procedure is applied to extract the watermarking information.

Procedure (1)

1. The 4x4 elements of each 8x8 block of the DCT matrix is extracted forming a new matrix, of quarter the original size,

2. The histogram is estimate for all the DCT coefficients of the generated matrix, excluding the first three LSBs (for integration purpose during authentication),
3. The histogram array is encrypted by (1),
4. Redundancy is eliminated from the generated array.

Now the watermark information is ready to be embedded into the shrunk quantized DCT matrix. The elements of the watermark array are embedded into the three LSBs of specified coefficients of that matrix. The first element of the watermark array is embedded into the LSBs of a certain coefficient that is chosen randomly. This element is remarked as 'modified', to not modify the same coefficient twice. Then the rest of elements are embedded by applying procedure (2).

Procedure (2)

1. Search the entire matrix until finding a coefficient equal to the previous element of the watermark array,
2. If it is found, store its x-position and y-position into the LSBs of the next (or previous, if the it is the image border) two pixels, remark these elements as 'modified',
3. Repeat step (2) until no more coefficients that is equal to current watermark element,
4. Get next element of the watermark array and go to step (1).

The procedure is repeated until all elements of the watermark array is embedded, or the block is skipped if the match could not be found. After that the matrix is resized back to the original size and the entropy coding takes place for transmission, as seen in Figure 3.

Before going further describing the rest of the proposed scheme, it is important to demonstrate a sample that mentions the reason of choosing the shrunk matrix size. It is expected that changes among pixels of the 8x8 block is small, and sometimes negligible. As it is seen in Figure 4, the DC coefficient of the DCT transformed block lies at the upper left corner and the rest are the AC coefficients. As it is shown, the 8x8 matrix corresponds to the quantized DCT matrix after rounding has many zeros and the first 4x4 elements holds the DC and the most important coefficients. That is why the proposed algorithm discarded the other elements.

3.2. The Proposed Scheme: Authenticating

200	202	189	188	189	175	175	175
200	203	198	188	189	182	178	175
203	200	200	195	200	187	185	175
200	200	200	200	197	187	187	187
200	205	200	200	195	188	187	175
200	200	200	200	200	190	187	175
205	200	199	200	191	187	187	175
210	200	200	200	188	185	187	186

(a)

515	65	-12	4	1	2	-8	5
-16	3	2	0	0	-11	-2	3
-12	6	11	-1	3	0	1	-2
-8	3	-4	2	-2	-3	-5	-2
0	-2	7	-5	4	0	-1	-4
0	-3	-1	0	4	1	-1	0
3	-2	-3	3	3	-1	-1	3
-2	5	-2	4	-2	2	-3	0

(b)

32	6	-1	0	0	0	0	0
-1	0	0	0	0	0	0	0
-1	0	1	0	0	0	0	0
-1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(c)

Figure 4. 8x8-pixels Block of an Image 'Lena' (a) Its gray levels, (b) Its DCT transformation, (c) After Quantization

The authentication process is applied by watermarking the received watermarked quantized matrix by the same way as applied at the sender side. If the extracted watermark information at the receiver is equivalent to the extracted watermark at the sender, and if it is embedded at the same locations as it is done at the sender side, then the received image is identical to the sent image and it is 'authenticated', otherwise it is 'not authenticated', as seen in Figure 5.

4. Developing the Proposed Scheme

The proposed authentication scheme is developed using MATLAB installed on Core™ i7-2.2GHz with 4 GB-RAM. The customized JPEG encoder/decoder is developed concerning the proposed watermarking and authentication processes that applied at the appropriate locations.

Fifty 'Bitmap' color images are downloaded from the internet and used for developing and evaluating the proposed scheme.

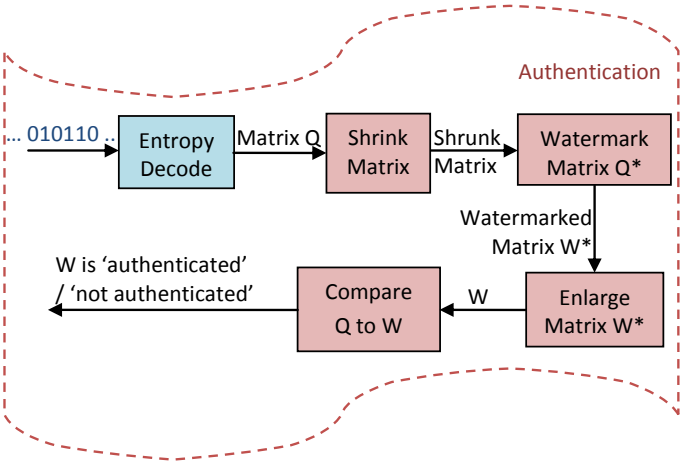

Figure 5. Block Diagram of the Proposed Authentication

The following steps are followed to develop the proposed scheme:

1. Color conversion is applied to convert the RGB model into YUV model, which separate the luminance component from the color components,
2. The luminance component is subdivided into non-overlapped 8x8 pixel blocks,
3. The DCT transformation is applied to each block,
4. The watermark information is extracted as described in Procedure (1),
5. The watermark information is embedded as described in Procedure (2),

In real system, the watermarked matrix is then encoded using a lossless entropy encoder to be transmitted. The other two color components are chromatic sub-sampled, DCT transformed, quantized, rounded, and then encoded and transmitted.

Once the luminance data is received, the authentication procedure takes place, as follows:

1) The received encoded data, as seen in Fig. 5, is set into matrix 'Q', and the watermark information is extracted from it by applying procedure (1),
2) The watermark information is embedded into the shrunk matrix 'Q*' by applying Procedure (2), generating matrix 'W*',

3) The watermarked shrunk matrix is enlarged to its original size, generating matrix W,

4) Compare 'W' to 'Q', if they are identical, the data is verified as 'authenticated', and the decompression process takes place, otherwise the data is manipulated and it is verified as 'not authenticated'.

4.1. The Proposed Scheme: Evaluation

In our previous work for authenticating uncompressed (or lossless compressed) images, the evaluation strategy depended on performing both geometrical and image processing attacks to the watermarked images directly, and then applying the proposed authentication scheme [24]. All attacked watermarked images are successfully verified as 'not authenticated'. That authentication scheme is fragile and blind, but not robust to un-malicious changes such as lossy compression.

The work proposed in this paper is fragile and blind too, but it is robust to lossy compression. Because the watermarking is applied just before transmitting the compressed encoded data, and authenticated once these data are received. Any slight changes of the transmitted data before it is received will be detected by the proposed scheme; even if it is just decompression (illegal decompression from unauthorized receiver).The authentication is performed before the legal decompression is applied by the authorized receiver. Any manipulation for the transmitted watermarked data before authentication at the authorized receiver will be detected by the proposed authentication scheme, as seen in Figure 6.

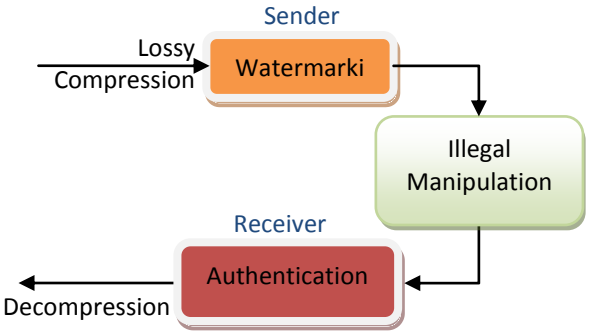

Figure 6. Block Diagram of the Proposed Scheme Concerning Illegal Manipulation

For evaluating the proposed scheme, it is important to proof that it is really fragile, blind, and robust to lossy compression. The scheme is developed, all testing image are watermarked, and then authenticated successfully as 'authenticated'. The proposed scheme is blind, because no information about the watermark or the original images is supported to the authentication procedure, as described in procedure (2).

Manipulating watermarked data is applied before and after decompression to proof that the proposed scheme is robust to lossy compression. This is done by manipulating 1) the watermarked quantized DCT matrices; and 2) the reconstructed watermarked images, and then the verification algorithm is applied. For manipulating the quantized matrix, their non-zero coefficients are down-scaled to half their values, and then the authentication algorithm is applied. In this case all matrices of all tampered images are verified successfully as 'not-authenticated'.

The reconstructed watermarked image is manipulated by modifying the MSBs of all pixels. In details, the quantized matrix that is watermarked is de-quantized, and

then the IDCT is performed. After that the image is manipulated by modifying the MSBs only, and then compressed and encoded again to be transmitted. The authentication algorithm is applied to the received data that is verified successfully as 'not-authenticated'.

The manipulation procedures are applied to all images of the testing set. Two watermarked images are seen in Figure 7-a, and 7-d of PSNR 38.17 dB, and 35.53 dB, respectively. The distortions of the watermarked images due to embedding the watermark are 0.17 dB and 0.07 dB, respectively. This is because the PSNR of the original images are 38.34 and 35.60, respectively. Figure 7-b and 7-e show the images after manipulating the quantized matrix. Figure 7-c and 7-f show the images after manipulating the MSBs. In all cases, the manipulated images are verified successfully as ‘not authenticated’.

4.2. The Proposed Scheme: Comparable Results

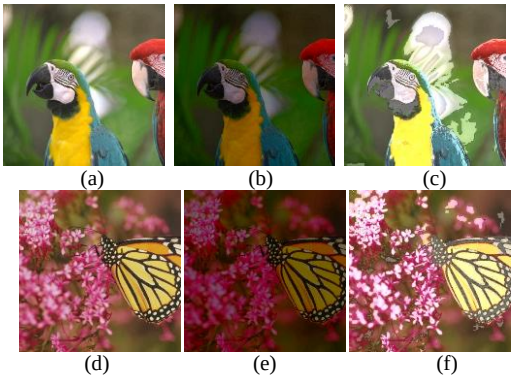

Figure 7. Samples of the Testing Images: (a), (d) Show the Watermarked Versions, (b), (e) Show the Manipulated Versions Due to Tampering the Watermarked Quantized Matrix, (c) and (f) Show the Manipulated Versions Due to Tampering the MSBs

PSNR (dB):

Original	**(a)**	**(b)**	**(c)**	Distortion (dB):
38.34	38.17	12.25	17.34	0.17
Original	**(d)**	**(e)**	**(f)**	
35.60	35.53	12.96	17.06	0.07

For further evaluating the proposed scheme, the results are compared to those in the reviewed literature. So that, several aspects should be considered; namely, image quality, automation, robustness, invertible, blindness, and fragility. The image quality concerns PSNR or Amount of Distortion (AoD) due to embedding the watermark information. The scheme is automatic if it does not depend on predefined parameters such as thresholds. The scheme is robust if it is capable of accepting un-malicious attacks, such as lossy compression and/or noise due to transmission over wireless channels. If the scheme is blind, there is no prior information is used to authenticate the received image. If any slight manipulation in the received image, even if it does not affect the image quality causes not to authenticate the image, this scheme is characterized as fragile. A scheme is either blind or inverted. Inverted scheme retrieves the original image before the watermark is embedded, so that the watermark information or the original image should be known for the receiver. In blind scheme, neither the watermark information nor the original image is needed for authenticating the received image. The predefined parameters, such as threshold,

are image dependant. However, using single value or even several values could not adapt for all images generated under different circumstances.

The mentioned aspects are used for comparing the proposed scheme with the related schemes reviewed in the literature. As seen in Table 1, the proposed scheme is fragile, blind, and robust against lossy compression, distorting the original images by only 0.063 dB, in average, due to embedding the watermark information, overcoming all results in the reviewed literature. This is because watermark is embedded into the LSBs of just few coefficients. For 512x512 image size, only 300 coefficients, in average, versus 6,5536 non-zero coefficients are modified by embedding the watermark. In other words, 300x3 bits versus 6,5536x8 bits are modified of the 8-bit luminance component of the JPEG images. Most images are of very high PSNR, *i.e.*, very low distortion. Hence, results of two benchmark images are seen in Figure 8, showing very low distortion that added to the watermarked images. On the other hand, the images of relatively low PSNR have low contrast. In other words, that kind of images have few high frequencies, as seen in Fig. 9-a, while the opposite is found in Figure 9-b, an image with many high frequencies and high PSNR. The chart in Figure 10 shows the distortions of all testing images, indicating that the distortion added due to embedding the watermark is negligible. The achieved results overcome all those in the reviewed literature.

Table 1. Comparison between the Proposed Scheme and Schemes Proposed in [15], [18], And [19]

		Proposed Scheme	[15]	[18]	[19]
AoD	**(dB)**	0.063	0	3	0.2
Automation	**Threshold used?**	N	N	N	Y
Robustness against	**lossy compression**	Y	N	Y	Y
	other un-malicious attacks	N	N	N	Y
Characteristics	**Invertible**	N	Y	N	Y
	Blind	Y	N	Y	N

(a) (b)

Figure 8. Two Benchmark Images. (a) Lena, (b) Peppers

PSNR (dB)	**(a)**	**(b)**
Original	36.66	35.07
Watermarked	36.59	35.02
Distortion (dB)	0.07	0.05

(a) (b)

Figure 9. The Distortion of Watermarked Images (a) 'Sailing' and (b) 'Mandaril', are 0.18 dB and 0.02 dB, Respectively

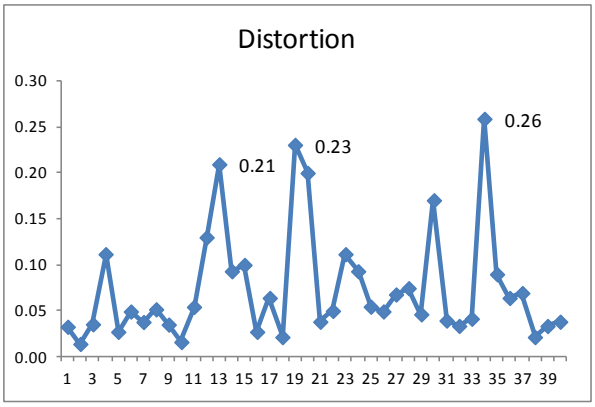

Figure 10. Distortion Chart for the Watermarked Testing Images, Indicating that the Distortion of Most Images didn't exceed 0.25 and the Majority is under 0.5

5. Conclusion

Robust authentication scheme is proposed in the presented work, handling the lossy compressed JPEG images. The images are watermarked and authenticated away from the heart of the compression and decompression processes. The watermarking procedure is applied to fifty testing images and then the authentication procedure is applied for verification. The scheme characteristics are evaluated by applying both the geometrical and image processing attacks to the watermarked images and then the authentication procedure is applied. The manipulated watermarked images are verified successfully as 'not authenticated'. Particular analysis are applied to the implemented scheme and further compared to similar schemes, indicating that the proposed scheme is fragile, blind, and robust to lossy compression. The achieved PSNR of the watermarked images is competitive. Further work will consider the authentication for compressed video streams taking into consideration robustness to image processing and geometrical transformations.

References

[1] Yao-Chung Lin, David Varodayan, and Bernd Girod, "Image Authentication Based on Distributed Source Coding," IEEE Transaction on Image Processing, Vol. 21, No. 1, Jan. (**2012**).

[2] Kostopoulos, I., Gilani, S.A.M., and Skodras, A.N., "Colour image authentication based on a self-embedding technique," 14th International Conference on Digital Signal Processing, IEEE (**2002**).

[3] Ee-Chien Chang, Mohan S. Kankanhalli, Xin Guan, Zhiyong Huang, and Yinghui Wu, "Robust image authentication using content based compression," Multimedia Systems © Springer-Verlag (**2003**).

[4] Xiaojun Qi, Xing Xin, and Ran Chang, "Image Authentication and Tamper Detection using Two Complementary Watermarks," 16th IEEE International Conference on Image Processing, ICIP'09. (**2009**).
[5] Mathias Schlauweg, Dima Pröfrock and Erika Müller, "JPEG2000-Based Secure Image Authentication," Proceedings of 8th workshop on Multimedia & Security, MM&Sec'06, September 26–27, Geneva, Switzerland. Copyright ACM (**2006**).
[6] Xiaoyun Wu, Junquan Hu, Zhixiong Gu, and Jiwu Huang, "A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters," ACSW Frontiers '05 Proceedings of the Australasian workshop on Grid computing and e-research - Volume 44, (**2005**) Pages 75-80.
[7] Małgorzata Steinder, Sami Iren, and Paul D. Amer, "Progressively Authenticated Image Transmisssion," Military Communications Conference Proceedings MILCOM, IEEE (**1999**).
[8] Liehua Xie and Gonzalo R. Arce, "Joint wavelet compression and authentication watermarking," International Conference on Image Processing Proceedings, ICIP'98. (**1998**).
[9] Liehua Xie and Gonzalo R. Arce, "A Class of Authentication Digital Watermarks for Secure Multimedia Communication," IEEE Transaction on Image Processing, VOL. 10, NO. 11, Nov. (**2001**).
[10] A. V. Subramanyam, Sabu Emmanuel, and Mohan S. Kankanhalli, "Robust Watermarking of Compressed and Encrypted JPEG2000 Images," IEEE Transaction on Multimedia, Vol. 14, No. 3, June (**2012**).
[11] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Secure Data Hiding in Wavelet Compressed Fingerprint Images," ACM Multimedia Workshop, Marina Del Rey CA USA, (**2000**).
[12] Osamah M. Al-Qershi1 and Bee Ee Khoo, "Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images," Journal of Digital Imaging, Springer, vol. 24, No 1, (**2011**) pp 114-125.
[13] Sonika C. Rathi and Vandana S. Inamdar, "Medical Images Authentication Through Watermarking Preserving ROI," Health Informatics - An International Journal (HIIJ) Vol.1, No.1, August (**2012**).
[14] Piper, A. and Safavi-Naini, R., "Scalable fragile watermarking for image authentication," Volume:7, Dec. (**2013**).
[15] K Pushpala, and R Nigudkar, "A Novel Watermarking Technique for Medical Image Authentication," Computers in Cardiology, IEEE, DOI:10.1109/CIC.2005.1588194. (**2005**).
[16] Mohammed Alkhathami, Fengling Han and Ron Van Schyndel , "Fingerprint image protection using two watermarks without corrupting minutiae," 8th IEEE Conference on Industrial Electronics and Applications (ICIEA), (**2013**).
[17] Hui Wang, Anthony T. S. Ho, and Xi Zhao, "A Novel Fast Self-restoration Semi-fragile Watermarking Algorithm for Image Content Authentication Resistant to JPEG Compression," Digital Forensics and Watermarking, Lecture Notes in Computer Science, Springer Link, vol. 7128, (2012) pp 72-85.
[18] Daxing Zhang, Shiming Liang, Zhigeng Pan, Haihua Li, and Xin Liu, "An Image Authentication Scheme Based on Correlation," International Journal of Digital Content Technology and its Applications Volume 4, Number 2, April (**2010**).
[19] Xiangui Kang, Jiwu Huang, Yun Q. Shi, and Yan Lin, "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression," IEEE Transaction on Circuits and Systems for Video Technology, Vol. 13, No. 8, Aug. (**2003**)
[20] Yu-Chen Hu, Chun-Chi Lo, Chang-Ming Wu, Wu-Lin Chen, and Chia-HsienWen, "Probability-based Tamper Detection Scheme for BTC-compressed Images Based on Quantization Levels Modification," International Journal of Security and Its Applications Vol. 7, No. 3, May, (**2013**)
[21] Luntian Mou, Tiejun Huang, Yonghong Tian, Shiguo Lian, and Xilin Chen "Robust and Discriminative Image Authentication Based on Sparse Coding," 7th IEEE International Workshop on Digital Rights Management Impact on Consumer Communications. (**2011**)
[22] A. Said, W. A. Pearlman, "A New Fast and Efficient Image Codec Based on Set Partitioning in Hierarchical Trees," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 6, June(**1996**) pp 243-250.
[23] Adil Haouzia, and Rita Noumeir, "Methods for image authentication: a survey," Multimedia Tools and Applications, Volume 39, Issue 1, August (**2008**) pp 1-46.
[24] Mona A. M. Fouad, and Ahmed Mokhtar A. M., "'Hop Horse' Image Authentication Scheme," International Journal of Multimedia and Ubiquitous Engineering (IJMUE) Volume 10, No. 5, May (**2015**).
[25] Ze-Nian Li and Mark S Drew, "Fundamentals of Multimedia," © 2004 by Pearson Education, Inc. ISBN 0-13-127256-X, (**2004**) pp 253-287.

