Perceptible Content Retrieval in DCT Domain and Semi-Fragile Watermarking Technique for Perceptible Content Authentication

CHAMIDU ATUPELAGE, KOICHI HARADA.
Department of Information Engineering,
Hiroshima University,
1-7-1 Kagamiyama, Higashi-Hiroshima, 739-8521.
JAPAN.
atupelage@hiroshima-u.ac.jp, harada@mis.hiroshima-u.ac.jp

Abstract: - Digital watermarking was commenced to copyright protection and ownership verification of multimedia data. However the evolution of the watermark focused on different security aspects of multimedia data such as integrity and authenticity. Fragile and semi-fragile watermarking schemes were introduced to accomplish these requirements. In this paper, we propose semi-fragile watermarking scheme to authenticate visual content of the image. The proposed method is carried out in DCT domain and authenticating the particular number of low frequency coefficient, it achieves the integrity of the image. Since low frequency coefficients carry the essence of the visual data, authenticating only the low frequency data is adequate. Therefore the proposed technique is efficient than the others, which are processing in all DCT coefficients. Digital signature is generated by following the definition of elliptic curve digital signature algorithm (ECDSA). Thus, the scheme is faster than RSA based authentication definition and it provides high level of security and availability. Additionally our scheme localizes the compromised area of the image. Embedded and visual data are protected from quantization of JPEG by altering the quantization table. However the degradation of compression ratio due to alternation in quantization table has been evaluated. Experimental results show that the watermark does not make any visual artifact in original data and it gives evidence that compression ratio degradation is ignorable for average JPEG quality factors.

Key-Words: - semi-fragile watermarking, public key cryptography, discrete cosine transformation, image authentication, imperceptibility, elliptic curve digital signature algorithm, JPEG.

1 Introduction

As the immense growth of the digital multimedia technologies, multimedia data creation and distribution have become very simple for the content owners. However illegal usage of multimedia data also has been increased such as copying and editing, facilitate unauthorized use, misappropriation and misrepresentation. Thus, the significance of protecting the integrity of the digital media elements and the intellectual property rights of its owners has became a great exertion among owners and content distributors. Digital watermarking is a promising approach for the content owners to defeat these substances. Initially, digital watermarking techniques were proposed as a solution for intellectual property right management and copyright management and those were considered as robust watermarking approachs. However evolution defined other types of watermark called fragile watermark that facilitates for integrity and authenticity of multimedia data. Fragile watermarks are highly sensitive for both malicious and non-malicious manipulations. In practice non-malicious manipulations are accepted, thus fragile watermarks are poor solution for real-time applications. This constrain has been defeated in semi-fragile watermarks, which robust against non-malicious manipulations and fragile for malicious manipulations.

In this paper we propose a new semi-fragile watermarking scheme which provides integrity and authenticity of the content of the images. The system is capable of localizing the tampered area. Inheriting the existing public key cryptography, the proposed scheme provides strong security. Most of the semi-fragile watermarking proposals use another image or random bit sequence as a watermark. However, if the attacker can safely alter the visual content without harming to the watermark, the watermarking scheme will certainly be failed (authenticating source as genuine). In our approach the watermark is a digital signature of the visual content of the image. Therefore this watermarking scheme is sensitive to visual content alternations such as cropping, replacing, etc.

In section 2 we will discuss the essence of semi-fragile watermarks and its features. Section 3

briefs existing multimedia authentication watermarking approaches and their limitations. Then we look into the system overview and design issues in section 4. Consequently we will discuss system definition and implementation issues in section 5 and 6. Simulation results will be presented in section 7. In section 8 we will present the analysis of the experimented results. Finally we conclude everything with future directions in section 9.

2 Semi-Fragile Watermarks for Image Authentication

Image and video authentication is applicable for e-commerce applications such as law, defense, journalism, and video conferencing etc, which are intended to show that no tampering has occurred during the situations where the credibility of an image or video may be questioned.

In fragile marking system, a signal (watermark) is embedded within an image such that subsequent alternations to the watermarked image can be detected with higher probability. Therefore fragile watermarking provides a promising approach for image and video authentication [1]. In history, fragile watermark authentication schemes intended to provide some set of common features. Our literature review of semi-fragile watermarking and multimedia security concludes a set of features which should incorporated in an effective semi-fragile watermarking scheme.

1. *Tamper detection*: alternations should be detected in higher probability and harmless (alternations which are not make considerable damages) alternations could be ignored.
2. *Perceptible content authentication*: watermarking scheme should be able to authenticate only perceptible content. Authenticating every detail in image will increase the system overhead.
3. *Localizing alternations*: the system should be able to localize the alternations. It might be the exact location or particular area.
4. *Perceptual transparency*: The watermark should not be visible under normal circumstances or it may not hide or scramble any information in an image.
5. *Large watermarking space*: the length of the watermark is proportional to the security strength; conversely large watermarks make visual artifacts. Therefore the watermarking scheme should select embedding domain which provide large space while maintaining minor artifacts.
6. *Robust to non-malicious attacks*: The watermark withstands to the predefined image manipulation technique. For example watermark should not be damage for trusted compression techniques such as JPEG or MPEG.
7. *Incorporate to PKI*: watermarking scheme should protect from common security attacks such as stego attacks, verification device attacks, key prediction attacks, etc. Incorporating to PKI will prevent these types of security attacks.
8. *Independent recovering*: recovery credentials should be independent from the watermark generation credentials except the keys. Systems where using same information in between both receiver and sender will be vulnerable for prediction attacks.

3 Related Work and Motivation

Min Wu and Bede Liu have proposed a watermark scheme for image authentication with localization. However inconsistent values of look-up-table may cause noise in the watermarked image [2]. Visible Watermarking and Verifiable Digital Seal Image [3] is a fragile watermarking approach which has integrated to PKI based digital signature algorithm. This method does not localize the tampering and the seal image may hide important visual information. [4] proposed a blind watermarking approach, which it tampers the alternation with localizing, but both parties have to share the same secrete credentials. Multimedia data authenticating method proposed in [5], which it uses original watermark at the authenticator, thus it does not fit with real-time applications. [6] is vulnerable to JPEG and it provides erroneous results for images having more edges and texts. Jessica proposed the new fragile watermarking approach in [7], though it is too fragile for a simple image processing technique. Embedding security is obliviously increases the overhead of the multimedia applications, thus it necessary to concern low processing overhead of the security integration. Using efficient DWT based spread spectrum, digital watermarking scheme was proposed in [15]: the algorithm has proposed as a parallel architecture to be minimized processing time. However, it processes in each pixel of the images, thus it implicitly increases the system overhead. Moreover, parallel architecture will not be

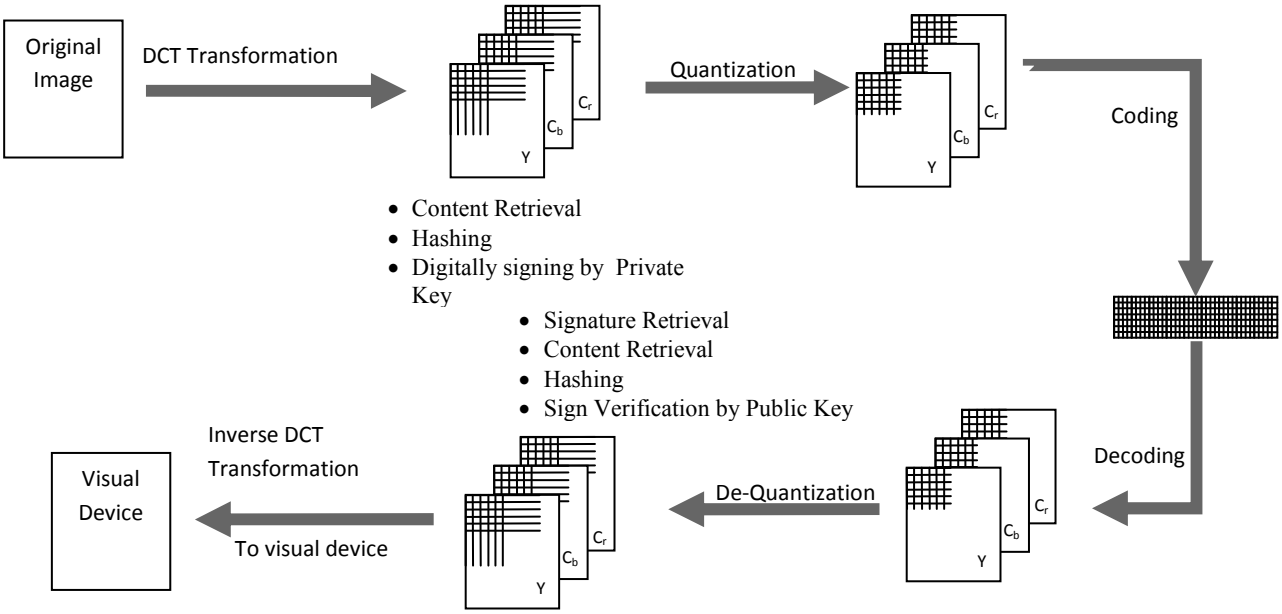

Fig. 1 Watermarking in JPEG encoding

applicable in most of the multimedia application due to its setup cost. Securing the communication of digital images, direct encryption and decryption algorithm has been proposed in [16]. In this algorithm, digital image becomes indistinguishable, after converting the pixel colors to logistic chaotic map. However the decryption requires mapping parameters and number of processing iterations which used in encryption. The major limitations of in this approach are system overhead due to work out in all pixels and difficulty of sharing the security credentials.

The literature review is evident that there is not any method has been proposed, which being able to fulfill the entire semi-fragile watermarking requirements. In this paper, we propose new content based effective semi-fragile watermarking scheme for image authentication and content verification.

4 System Overview & Design Issues

Lossy compression algorithms discard the information in digital assets which are not perceived by HVS (Human Visual System). It is apparent; authenticating all information in an image will increase the computational cost and complexity. Therefore this approach only authenticates the perceptual information in an image. Also this technique is robust against the JPEG compression, and sensitive for the threats such as content removal, visual information deformation, cropping, etc.

DCT domain is desired to be used to retrieve visual content and embed the watermark, thus the verification is also carried out in the same domain. Watermark (digital signature) is generated from the retrieved visual content and it will be embedded into the image. To keep the signature safe from the compression, we concern the invariant properties in particular compression system. In the simulation of our scheme, we concern JPEG compression, because it is widely used and JPEG compression techniques are used as basis for some popular video compressions.

JPEG lossy compression algorithm consists of three major processors, which are DCT computation, quantization and variable length code assignment [8]. Fig.1 depicts how proposed system collaborates in JPEG compression scheme. When JPEG reaches in DCT domain, the visual content is retrieve and generated the digital signature and embedded it in the selected low frequency coefficients. Similarly authentication routines are also carried out after de-quantization (before send to the visualization) as shown in Fig.1. Verification routines include retrieval of embedded signature and visual content, and then the content is verified against to stored digital signature.

4. 1 Visible Content Retrieval

Due to the immensity behavior, multimedia data always anticipates some compression; however transform domain compression techniques have become popular. The most popular and currently use transform domain techniques are discrete cosine transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT). Therefore transform

domain watermarking techniques also have been become popular, because such watermarking techniques can avoid computational cost of domain transformation. For more information refer [2], [3] for DCT based watermarking and [13], [14] for DWT based domain. However at current, DCT based compressions can be consider as widely used, because popular H.261/2/3, MPEG-1/2/4, HDTV and CMTT.723 are based on DCT based transformation. Therefore in our scheme we choose DCT domain as transformation domain. Recipient of digital media always anticipate the assurance of the content integrity than the degradation of quality (Ex: JPEG and MPEG). If some attack does not alter the important visual content recipient might accept it, because of the recipient may satisfy from existing information. (Ex: identifying face in the image in spite of its quality).

JPEG discards the information which cannot be perceived under ordinary conditions. Analysis of DCT coefficients concludes lower frequency coefficients are carrying more than half of the visual information in an image. Li Weng and Bart Preneel [9] has precisely benchmarked that 60% of the visual information conserved in the DC coefficient and 70% of visual information is drawn to DC and first two AC coefficients (in order to zigzag scanning in 8×8 pixels block). In Fig. 2, right side image (b) has been generated by removing all AC coefficients of DCT domain of left side image. Though it can be identified the

(a) Original Image (b) After removing all AC coefficients

Fig. 2: Visual information preserve in DC coefficient

content of the image.

Therefore authenticating only DC coefficients or DC with first two AC coefficients, we can assure the authenticity of 60% or 70% of the visual content respectively. In our proposed scheme the visual content can be considered as a variable where user can decide the authenticity level of the application.

Table 1: Comparison of key lengths of different security definitions (Taken from [10])

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

4.2 Security Infrastructure

According to the definitions in PKI, the key length is an important factor than the secrecy of the algorithm. Therefore key length is an important factor in this research and it proportional to the signature length and the large watermarks intuitively increases the noise. Elliptic curve digital signature algorithm (ECDSA) is a promising approach to overcome this limitation, which provides maximum security even smaller key length. The remarks and the benchmarks of the security of the elliptic curve cryptosystem are available in [10]. Table 1 gives comparison of key lengths of different security protocols and it gives an evidence of significance of using elliptic curve cryptography in our definition.

Following we will briefly illustrate the definition of ECDSA.

Notation:

n : Order of and elliptic curve
G : Base point of an elliptic curve
d : Signer's private key
Q : Signer's public key
H : Hash function

ECDSA Signature Generation:

To sign a message m, an entity A with domain parameters and associated key pair (d, Q) does the following (where $Q = dG$)

1. Select a random or pseudorandom integer $k, 1 \leq k \leq n-1$.
2. Compute $kG = (x_1, y_1)$ and convert x_1 to an integer $\overline{x_1}$.
3. Compute $r = x_1 mod\, n$. If $r = 0$ then go to step 1.
4. Compute $k^{-1} mod\, n$.
5. Computer $H(m)$ and convert this bit string to an integer e.
6. Computer $s = k^{-1}(e + dr)\, mod\, n$. If $s = 0$ then go to step 1.
7. A's signature for the message m is (r, s).

ECDSA Signature Verification:
To verify A's signature (r, s) on m, B obtains an authentic copy of A's domain parameters and associated public key Q. Then B does the followings,

1. Verify that r and s are integers in interval $[1, n-1]$.
2. Computer $H(m)$ and convert this bit string to an integer e.
3. Compute $w = s^{-1} \bmod n$.
4. Compute $u_1 = ew \bmod n$ and $u_2 = rw \bmod n$.
5. Compute $X = u_1 G + u_2 Q$.
6. If $X = O$, then reject the signature. Otherwise convert the x-coordinate x_1 of X to and integer $\overline{x}_1$, and computer $v = \overline{x}_1 mod\ n$.
7. Accept the signature if and only if $v = r$.

Proof that Signature Verification Works:
If the signature (r, s) on message m is generated by A, then $s = k^{-1}(e + dr) \bmod n$.
Thus,
$u_1 G + u_2 Q = (u_1 + u_2 d)G = kG$, and so $v = r$ is required.

Our security architecture assumes content owner distributes his/her public key at some secure certificate server with digitally signed certificate. Private Key is kept secure and it is used to generate the signature. Content receiver use corresponding public key for signature verification.

5 System Definition

In this section we will explain two main intermediate routines of the proposed scheme. Firstly, we will express the routines of watermark (signature) generation and embedding in DCT domain, and then secondly watermark retrieving and verification routines are illustrated.

These basic notations are used in following two sections for easy representation.

- I_s : Source image.
- I_w : Watermarked image.
- $F_{RET}()$: Retrieving the visual content.
- $F_{INS}()$: Embedding the signature.
- $F_{EXT}()$: Extracting the signature.
- $H_{MD5}()$: Hash function.
- K_{PR} : Signer's private key.
- K_{PU} : Signer's public key.
- s : Signature.
- md : Message digest.
- vc : Visual content.
- $ECDSA()$: ECDSA function

5.1 Signature Generation and Embedding

At first, the system should retrieve the desired visual content and preprocess (Arranging predefined manner). Hashing function generates the message digest from the visual content and this digest is sent to the signature generating algorithm (ECDSA) together with signer's private key. In order to our definition the watermark is the digital signature of the visual content. The signature is embedded into the image at the same frequency domain. The whole procedure can be represented as algorithmically as follow.

1. $vc \leftarrow F_{RET}(I_s)$
2. $md \leftarrow H_{MD5}(vc)$
3. $s \leftarrow ECDSA(K_{PR}, md)$
4. $I_w \leftarrow F_{INS}(I_s, s)$

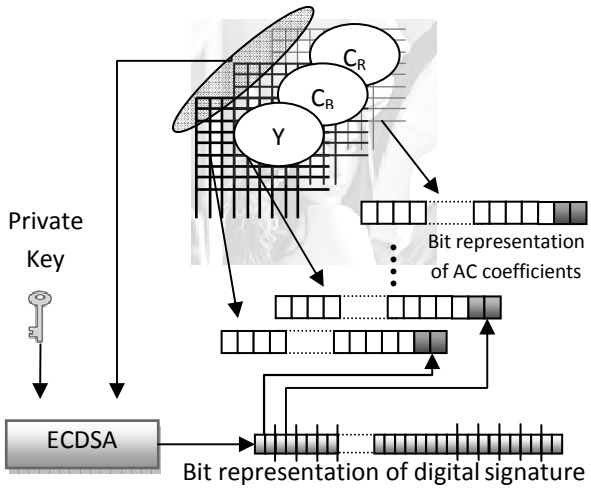

Fig.3: Signature generation and embedding (bit representation)

Fig.3 gives detail graphical representation of digital watermark generation and embedding routines. In DCT domain luminance and chrominance color channels (YCrCb) are considered independently and transformation is carried for blocks of 8×8 pixels (Macro Block). Message digest for DC coefficients is generated by hashing function. Then the message digest together with the private key are sent to the ECDSA and it returns digital signature (digital watermark). Generated digital signature is divided into two bit pieces and each piece replaces the least two significant bits of AC coefficients. This embedding procedure only carried out for selected number of AC coefficients in DCT domain (first 15 coefficients).

5.2 Signature Extraction and Verification

In the process of authentication, the visual content is retrieved from DC coefficients and will be sent to the hashing function to get the message digest. Signature (watermark) is recovered from LSBs of the AC coefficients and the signature verification expects three parameters; message-digest, original signature and public key, then it will return the validity of the signature according to the accuracy of the input parameters. The whole process can be illustrated as algorithmically in four steps.

1. $vc \leftarrow F_{RET}(I_w)$
2. $s \leftarrow F_{EXT}(I_w)$
3. $md \leftarrow H_{MD5}(vc)$
4. $ECDSA(K_{PU}, md, s) \rightarrow Acceptance$

Fig.4 is the graphical representation of the watermark retrieval and verification routines. The watermark is retrieved from the LSBs of AC coefficients and the visual content is retrieved from the DC values. Sending the message digest together with public key and the watermark, ECDSA returns the authenticity of the watermarks image.

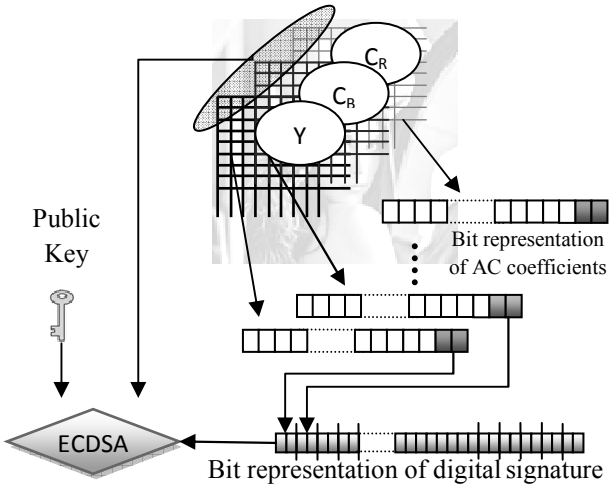

Fig.4: Signature retrieval and verification (bit representation)

6 Implementation Issues & Conquerors

In this section we will discuss the practical issue occurred at the implementation of this scheme and the defeating of them.

6.1 Altering Quantization Table

In general, coefficients in low frequency area of DCT domain capture the "essence" of the image. The high frequency area captures the fine details of the image. Most of the proposed watermarking schemes are interested of embedding the watermark in low frequency area in an image. However, in lossy data compression techniques, the coefficients are vulnerable in quantization process. However, there are several watermarking techniques have been proposed, which overcome this limitation by altering the quantization table [12].

In our approach, we marked selected low frequency coefficients as 1 (refer Fig.5 (a)) in order to zigzag scanning. Intuitively this alternation affects on the final compression ratio of the image. In this research the compression ratio degradation due to the alternation of quantization table is evaluated and the numerical details give an evident that degradation of compression ratio can be negligible.

6.2 Minimum Security Block Size

In most cryptographic functions, the key length is an important security parameter. However standard security organizations (such as ECRYPT, NIST) release specification for the key lengths of different security protocols. At present, NIST (National Institute of Standard Technology) recommendation for ECC key length as 160 bits and the corresponding signature length become 336 bits long [11]. Our proposed scheme, AC coefficients are carried the signature. Precisely, one 8×8 pixels block gives 14×2 bits (2 LSBs from 14 AC coefficients) space (more than 14 coefficients affects in compression ratio immensely) and including three channels it becomes 14×2×3 = 84 bits. Considering four blocks together (refer Fig.5) we can increase the space up to 84×4 = 336 bits. It is an adequate space for digital signature (watermark). According to this behavior, the minimum authentication block size will become 16×16 pixels instead of 8×8 pixels block. However 16×16 pixel block is still small to HVS and it can be considered as sufficient block size to authenticate.

6.3 Integrity of Perceptual Information

If someone expects to provide higher integrity (more than 60%) then AC coefficients are required to be fed into signature generation. However in our approach we explicitly replace two LSBs in low frequency AC coefficients (Fig.3). This makes intentional misrepresentation in digital signature. We overcome this limitation by separating AC bit sequence into two portions (refer Fig.5 (b)), where

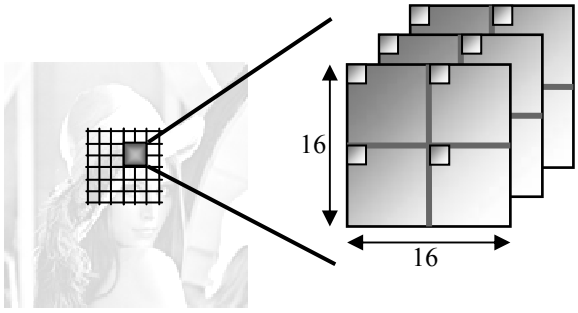

Fig. 5 Authentication block represent in source image

one portion is for authentication and the other is for carrying the signature. More precisely signature of the left portion is embedded in to right portion. However the left portion of the sequence holds considerable amount of information compared to the entire bit sequence. Therefore even avoiding 2 LSBs in AC coefficient we can acquire adequate authentication of the visual content.

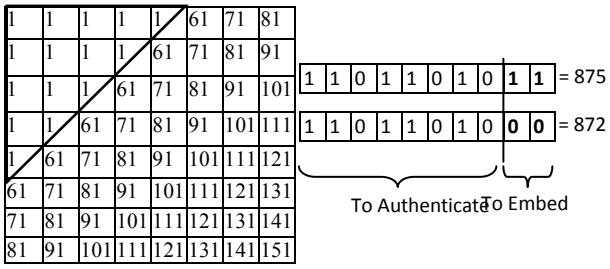

Fig. 6 (a) Quantization Matrix (b) Bit representation of AC coefficient

7 Simulations and Results

To prove the merit of our proposed scheme, we have carried out few experiments and its results are presented in this section. In the first experiment we evaluate the degradation in compression ratio due to the alternations in quantization table. Second experiment was carried out to evaluate the visual quality degradation due to watermark insertion.

In JPEG, quantization contributes considerable endeavor to the compression ratio. Conversely the proposed scheme alternates the quantization table

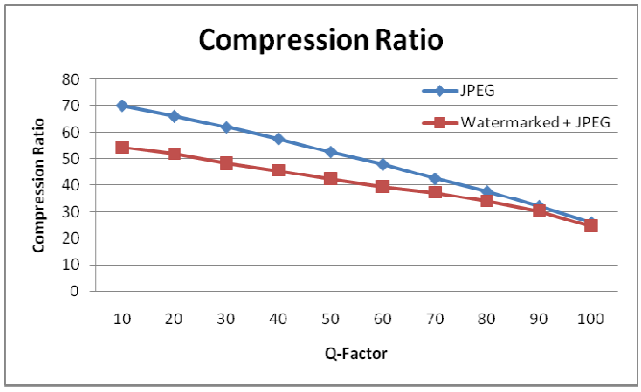

Fig.7 Comparison of compression ratios of JPEG and watermarked JPEG images

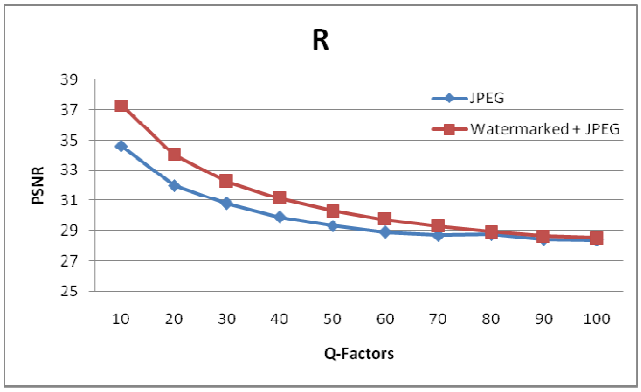

Fig.8 PSNR comparison of JPEG compressed and watermarked image for R

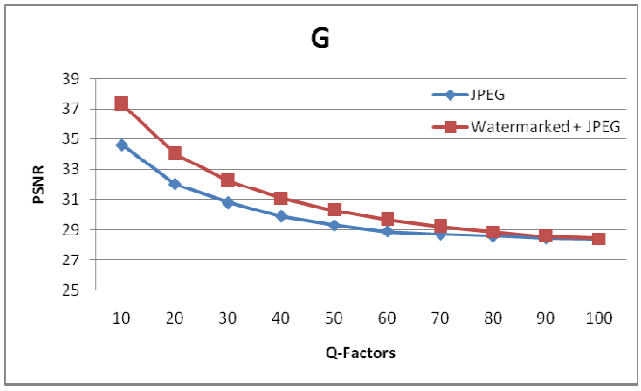

Fig.9 PSNR comparison of JPEG compressed and watermarked image for G

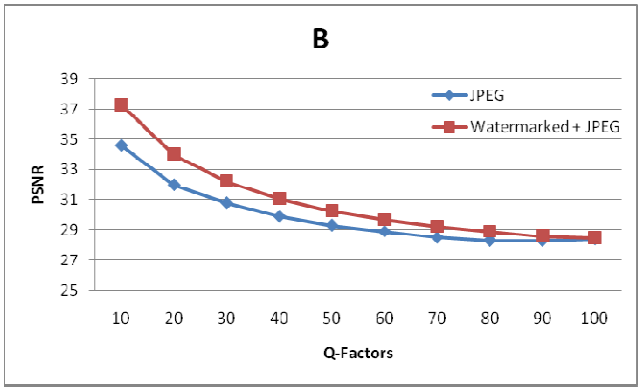

Fig.10 PSNR comparison of JPEG compressed and watermarked image for B

and this promises significance degradation in compression ratio of the resulted image. In our definition, 15 AC coefficients are altered. Moreover, quality factor (QF) in JPEG also provides significant contribution over quantization. Therefore in our first experiment, we measure the compression ratios of altered quantization process and non-altered quantization process against to the different quality factors vary from 10 to 100. We carried out the process over 20 images for each quality factor and average compression ratio has been plotted in Fig.7. For lower quality factors, compression ratio drop is around 21%, contrarily for higher quality factors it become less than 5%. However neither quality factor 10 nor quality factor 100 is used in practice, because of its low quality and less compression behavior respectively. However, for average quality factor (50), the compression ratio degradation is around 12 %. It is an evident that for practically applicable quality factors, the compression degradation is less. Therefore, the compression ratio degradation can ignored for average quality factors, concerning advantage gain for the security.

Embedding extra signal (watermark) into a host signal intuitively degrade the quality of the original source image. Our second experiment was carried out to quantify this quality degradation. In this experiment we took 11 bitmap images and compressed them following standard JPEG algorithm for the quality factors from 10 to 100 increased by 10 (10, 20,.., 100). Then we compressed the same bitmaps using our approach by inserting the watermark. Then we compare the watermarked compressed and non-watermarked compressed images for corresponding quality factors. We assess the quality distortion in two ways; as subjective assessment: we explicitly visualize the images and as objective assessment: we calculate the PSNR (peak signal-to-noise ratio) of the images. The comparison is carried out for each color components in RGB color model. Fig.8 presents the average PSNR values of red color component of 15 images in different quality factors. Similarly Fig.9 and Fig.10 represents the average PSNRs of green and blue color components. Considering the figures 8-10, PSNRs of the watermarked and non-watermarked images are very close at higher quality factors low compression); conversely PSNRs of the watermarked images exceed the non-watermarked images at lower quality factors. More precisely, quality of the watermarked images is better than non-watermarked image for low quality factors (large compressions). The reason for that is the quantization is higher for low quality factors and it is prevent by alternations in quantization table. Therefore it is an evident that watermark embedding does not make any harm for visual quality of the original sources.

As a subjective quality evaluation we have presented experimental results of parrot's image in Fig.11. It shows a comparison of JPEG compressed and watermark embedded compressed images for different quality factors. It gives an evident that for the low quality factors, quality of the watermarked image is significantly higher than JPEG images. However when the quality factor is increased, the quality of the watermarked image is in line with the quality of the JPEG image. Furthermore, Fig.11 proofs validity of the graphs plotted in Fig. 8 to 10.

8 Analysis & Discussion

In this section we present the analytical information of the proposed watermarking definition.

The major objective of this research is to accomplish a set of requirements (defined in section 1) that required to be achieved to be an effective fragile watermarking scheme. Table 2 summarizes those requirements with statuses of our achievement.

Table 2: Features of effective semi-fragile watermarking scheme

Requirement	Status
Tamper detection	Satisfied
Perceptible content authentication	Satisfied
Localizing alternation	Satisfied
Perceptual transparency	Satisfied
Large watermarking space	Satisfied
Robust to non-malicious attacks	Satisfied
Incorporate to the PKI	Satisfied
Independent recovering	Satisfied

The proposed fragile watermarking scheme detects any tampering, which is being effected on DC coefficient or DC with first two AC coefficients. More precisely proposed scheme can be use to authenticate 60% or 70% of the visual information of the images, conversely imperceptible alternations are smoothly avoided. The system can identify the compromised block mutually; locating the tampered block of size 16 $\times$16 pixels. We have evidently proved that the proposed scheme is transparent under normal visual observation in HVS. By choosing the frequency domain we have offered large space for

embedding the signature. Watermark embedding is proceeding before quantization in JPEG compression and the watermark is preserved in JPEG compression. In security point of view, our approach follows the digital signature authentication routines, and collaborating to the ECDSA, the proposed system takes advantage of smaller key length. Therefore, the system is strong against to the common security threats such as secret credential prediction. Because of the PKI based security infrastructure, the authenticator is completely independent from sender's information except the public key.

Q-factor	JPEG	JPEG + Watermark
30		
40		
50		
60		
70		

Fig. 11 Comparison of JPEG and Watermarked JPEG images of different quality factors.

9 Conclusion and Future Directions

A secure systems does not need to be perfect, however high enough degree of security should be reached. In other word watermark breaking does not need to be impossible, but only difficult.

Our literature review defined a set of features, which should be achieved by an effective semi fragile watermarking scheme. In this paper we proposed an effective fragile watermarking scheme, which accomplishes all defined requirements. In this paper we precisely discussed designed aspects, issues and conquerors, and implementation details. Experimented results prove the essence of the proposed scheme.

Our future directions include: 1) More detail evaluation of the performance of the scheme, 2) More precise analysis of security attacks and survivability of the watermark, 3) applying same directions for MPEG and JPEG2000 definitions.

References:

[1] Lin E T, Delp E J. A review of fragile image watermarks. *Multimedia and Security Workshop (ACM Multimedia'99),* Orlando, 1999, pp. 25-29.

[2] Min Wu, Bede Liu, Watermarking for Image Authentication. *International Conference on Image Processing (ICIP),* 1998, pp. 437-441.

[3] Hyuncheol Park, Kwangjo Kim,Visible Watermarking using Verifiable Digital Seal Image, *Symposium on Cryptography and Information Security*, Japan,2001, pp. 103-108.

[4] J.J. Eggers, and B.Girod, Blind watermarking applied to image authentication, *IEEE International Conference on Acoustics, Speech and Signal Processing,* Vol. 3, 2002, pp. 1977 - 1980.

[5] Ming-Shing Hsieh, Din-Chang Tseng, Perceptual Digital Watermarking for Image Authentication in Electronic Commerce, *Kluwer Academic Publishers Norwell*, MA, USA, 2004, Vol. 4, pp. 157 - 170.

[6] Eugene T. Lin, Christine I. Podilchuk, Edward J. Delp, Detection of image alterations using semi-fragile watermarks, *SPIE proceedings series*, San Jose , 2000., Vol. 3971, pp. 152-163.

[7] Jessica, Fridrich, Security of fragile authentication watermarks with localization, *SPIE proceedings series*, Bellingham, 2002, Vol. 4675, pp. 691-700.

[8] Wallace, G.K., The JPEG still picture compression standard. *IEEE Transactions on Consumer Electronics*, 1992, Vol. 38, pp. xviii - xxxiv.

[9] L. Weng, B. Preneel, On encryption and authentication of the DC DCT coefficient, *International Conference on Signal Processing and Multimedia Applications*, 2007.

[10] Certicom, The Elliptic Curve Cryptosystem, http://www.comms.scitech.susx.ac.uk/fft/crypto/EccWhite3.pdf, 2000.

[11] Keylength.com, http://www.keylength.com/en/compare/

[12] Ching-Tang Hsieh, Yeh-Kuang Wu, A Watermarking System Based on Complementary Quantization, *Proceedings of the 6th WSEAS International Conference on Signal, Speech and Image Processing*, Lisbon, Portugal, September 22-24, 2006, pp. 7-10.

[13] XUN WANG, YI OU-YANG, AND HUA-MAO GU, A remote sensing image self-adaptive blind watermarking algorithm based on wavelet transformation, *Proceedings of the 7th WSEAS International Conference on Signal, Speech and Image Processing*, Beijing, China, September 15-17, 2007.

[14] KITAE YOON, SINHYUK CHOI, SEUNGSOO BAE, HUIGON KIM, JINSEON YOUN, TANAM THANG, JUNRIM CHOI, Adaptive Block Watermarking and its SOC implementation Based on JPEG2000 DWT, *Proceedings of the 7th WSEAS International Conference on Signal, Speech and Image Processing*, Beijing, China, September 15-17, 2007.

[15] Ali Sasan, M. Shamim Baig, Parallel Implementation of Spread Spectrum Based Oblivious Visual Watermarking Using Efficient DWT. *Proceedings of the 6th WSEAS International Conference on Applied Computer Science,* Tenerife, Canary Island, Spain, December 16-18, 2006.

[16] A. N. Pisarchik, N. J. Flores-Carmona, Computer Algorithms for Direct Encryption and Decryption of Digital Images for Secure Communication, *Proceedings of the 6th WSEAS International Conference on Applied Computer Science,* Tenerife, Canary Island, Spain, December 16-18, 2006.