Recognizing Image Authenticity using DCT based Watermarking

Jayashree S Pillai
Research Scholar
Mother Teresa Women's University, Kodaikanal

Padma T
Professor,
Sona College of Technology, Salem

Ambili P. S
Asst. Professor
SAINTGITS College of Engineering, Kottayam

ABSTRACT

The authenticity of the watermarked images under various incidental noise is considered in this paper. The watermark is generated using from the content invariant properties of the image and securely embedded in the selected higher textured blocks of the DCT transform of the image to make them robust to jpeg compression and incidental distortions. Response of the authenticator to watermarked images subject to various incidental attacks and compression is evaluated to test the suitability of the scheme to achieve selective authentication.

Keywords

Authentication, PQ Sequences, Feature vector, Key vector, textured regions, content based watermark.

1. INTRODUCTION

Authentication of digital media is the verification of the integrity of the media or asserting its copyright. With increased requirement for storing and transmitting information and the availability of advanced image processing tools, techniques are essential to establish the copyright and/or integrity of the image. This can be achieved using signatures or by watermarking. In certain applications like healthcare, defence, evidence or artistry, it is important that the quality of the watermarked media is retained and at the same time it is robust to malicious manipulations.Digital watermarking [1][2][3][4][5] is a technique commonly used for authentication of media where the watermark is hidden in the media and later recovered to verify the identity of the owner or integrity of the media i.e., its authenticity. Any authentication process is incomplete without the use of a pseudo random pattern or key/keys to introduce randomness so as to increase the robustness of the procedure. This key is normally generated using any of the well known pseudorandom generators like the Linear Congruential Generator (LCG) or Blum Blum Shub Generator (BBS). In mathematics, a continued fraction is defined in [20][21][22] as an expression obtained through the iterative process of representing a number as the sum of its integer part and the reciprocal of another number, then writing the other number as the sum of its integer part and another reciprocal, and so on.

Authors in [11] generated the watermark derived using mathematical invariant relationship of corresponding DCT coefficients between a pair of blocks before and after JPEG compression and selected it as the image feature. [3] proposed a JPEG quantization property for all further smaller quantization tables to authenticate an image. [12] presented a scheme to verify the authenticity of JPEG images using secret keys and a mapping vector to embed the signature. The authors in [19] proposed improvements to the method in [11] using two properties Quantization Sum Invariant Property (QSIP) and Further Quantization Property (FQP) that always exist under JPEG compression. QSIP is used to extract the content based feature and embedded in the DCT coefficients. The verification is done using FQP. The authors in [24] and [25] have proposed watermarking using d-sequencesIn this paper the semi fragile watermarking procedure that is highly robust to Jpeg compression up to pre defined levels is proposed and the robustness to various incidental attacks is evaluated. The watermark is secured using pseudo random sequence generated from PQ Sequences [23] [26] and is embedded in the higher textured block selected from the block pair.

2. PROPOSED SCHEME

The authentication procedure has four stages - 1) Generation of the PQ sequence 2) Generation and scrambling of the watermark 3) Watermark insertion and 4) Watermark verification.

2.1 Generation of PQ sequences

A secret irrational number α is selected as a seed. The continued fraction expansion of α generates infinite partial coefficients which are processed to generate the PQ sequences. The generated sequence has been tested for randomness using various statistical tests in [26]. The Key Vector KV is extracted from the PQ sequences and is used to scramble the watermark for improved security.

2.2 Watermark Generation and scrambling Algorithm

Considering a pair of blocks (p, q), the relationship between two quantized DCT coefficients $\mathrm{DCT_p}(\mathrm{v})$ of block p and $\mathrm{DCT_q}(\mathrm{v})$ of block q at the same coordinate position v will remain the same before and after compression [17]. The same concept is used for generating the content based watermark. The algorithm for watermark generation is:

a) Compute DCT of 8x8 non-overlapping blocks. Also compute texture value $\mathrm{T}(\mathrm{p}, \mathrm{q})$ for each block and sort.
b) Place blocks in into two disjoint groups A and B based on a secret value and form pairs of blocks (p, q), using one from group A and the other from group B
c) For each pair of blocks (p, q),
 i. Select the top n low frequency DCT coefficients, which includes the DC coefficient and $\mathrm{n}-1$ low frequency AC coefficients. The feature vector $\mathrm{FV_{pq}}(\mathrm{v})$ is computed.

$$\mathrm{FV_{pq}}(\mathrm{v}) = \begin{cases} 1 & \text{if } \mathrm{DCT_p}(\mathrm{v}) \geq \mathrm{DCT_q}(\mathrm{v}) \\ 0 & \text{if } \mathrm{DCT_p}(\mathrm{v}) < \mathrm{DCT_q}(\mathrm{v}) \end{cases} \quad (1)$$

$$\text{for } v = 1..n$$

ii. Scramble $\mathrm{FV}_{pq}(v)$ by XORing with the corresponding Key Vector KV to get $\mathrm{SFV}_{pq}(v)$.

d) Steps c is repeated for all the pairs of blocks to obtain the SFV for each pair of blocks.

2.3 Watermark Insertion

The embedding is done in the high mid frequency coefficients of the higher textured block among the block pair to ensure robustness to lossy compression and at the same time exploit the HVS properties to minimize distortion.

Algorithm

For each pair of blocks (p,q)

The coefficients $C(a_i, a_{i+1}, \ldots \ldots a_m)$ from mid frequency region is selected for embedding. PQV is the chosen string of bits from the PQ sequence and those coefficients from C are selected where $PQV(j) = 1$.

Scrambled Feature Vector $SFV(v)$ decides on the watermark embedding. The difference of corresponding DC coefficients $DDC(v)$ is selected as the watermark and embedded into the selected mid frequency coefficients, after quantization, where the corresponding $SFV(v) = 1$ as follows:

$$\mathrm{WDCT}_{(p|q)}(v) = \begin{cases} \mathrm{DCT}_{(p|q)}(v) + \rho * \mathrm{DDC}(v) & \text{if } \mathrm{SFV}(v) = 1 \\ \mathrm{DCT}_{(p|q)}(v) & \text{otherwise} \end{cases}$$

where $\mathrm{WDCT}_{(p|q)}(v)$ represents the watermarked DCT coefficient of block pair (p, q), $\mathrm{DCT}_{(p|q)}(v)$ is the original DCT coefficient, and ρ is the watermarking strength. ρ is the ratio of standard deviation of the selected mid frequency coefficients to the standard deviation of the selected low frequency DCT coefficients, selected for feature vector extraction.

a) Inverse DCT of the image is computed to get the watermarked image.

2.4 Watermark extraction and authentication

At the receiving end, the watermarked image is verified for authenticity by a procedure similar to the embedding process-

a) Generate PQ sequence from the secret irrational number and extract the required pseudorandom vectors $KV^{\sim}$ and $PQV^{\sim}$ as mentioned in section 2.1 and 2.2 respectively.
b) Calculate $\mathrm{FV}^{\sim}$ from the DCT of 8*8 pair of blocks of watermarked image and XOR with Key Vector $KV^{\sim}$ to get $\mathrm{SFV}^{\sim}$, the scrambled feature vector as in section 2.2.
c) Extract the embedded difference of selected DC Coefficients $\mathrm{DDC}^{\sim}(v)$ and compare with the computed difference $\mathrm{DDC}^{*}(v)$. If $\mathrm{DDC}^{\sim}(v) - \mathrm{DDC}^{*}(v) < \tau$, then the block can be considered authentic, else tampered. τ is a user defined value that can be determined based on the level of authentication required and the image to be watermarked.

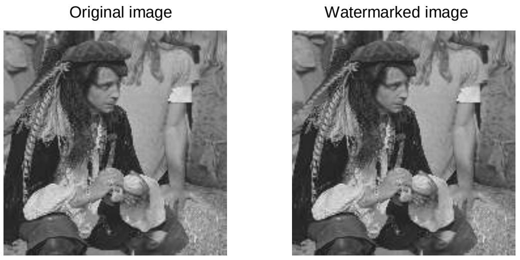
3. EXPERIMENTAL RESULTS

The proposed scheme was implemented using Matlab and standard test images were watermarked and evaluated for imperceptibility and robustness against incidental noise and jpeg compression.

3.1 Imperceptibility analysis

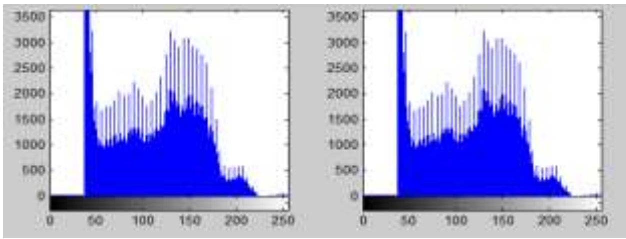
3.1.1 Quality of the watermarked images

The quality of images may be expressed in terms of mathematically proven measures like the change in the pixels of original and watermarked representation of the images or subjectively in terms of Human Visual System (HVS) models that are based on visual appearance or perception. The application determines the level of quality that is desired. The exactness of the watermarked image with the original in applications like medicine, military and court room evidence is expected to be very high due to the nature of the requirement. The quality of the watermarked images with respect to the original image can be measure in terms of Peak Signal to Noise Ratio (PSNR), Pearson Correlation Coefficient (PCC), Mean Square Error (MSE) and Structural Similarity (SSIM).Since the watermarking is carried out in the DCT domain where the mid frequency coefficients of the selected pair of blocks are modified to embed the watermark, the watermark is highly imperceptible and is reflected in Figures 1 and its histogram in Figure 2. The average PSNR value of the original and watermarked image is above 50 dB (decibels) which indicates high imperceptibility and the SSIM and PCC values are very close to 1 for some standard images - Table 1. All the measures indicate good quality of the images after watermarking.



(a) (b)

Figure 1 : a) Original Image b) Watermarked Image



(a) (b)

Figure 2: Histogram of the a) Original Image b) Watermarked Images

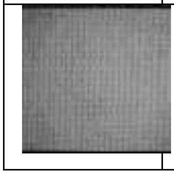
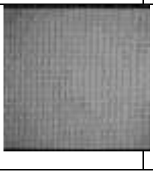
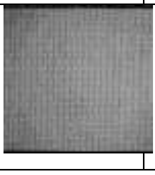
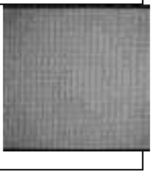
Table 1: Measures of imperceptibility of watermarked images of proposed technique

Watermarked Image	MSE	SSIM	PCC	PSNR (dB)
Lena	0.215	0.99	1	55
Rice	0.166	0.99	1	53
Pattern	0.318	0.99	1	53
Pentagon	0.010	0.99	1	52
Pirate_512	0.013	0.98	1	52
Cameraman_512	0.14	0.99	1	51
Drawing Room_512	0.117	0.99	1	50
Average	**0.139**	**0.99**	**1**	**52**

3.2 Tolerance to JPEG Compression

It is very common to compress images prior to storage and transmission and the authentication scheme is expected to be tolerant to common image compression methods. Feature Vector $FV_{pq}(v)$ is generated from compression tolerant features using Lin's Model [11] where the relationship between coefficients remains unchanged before and after compression. The tolerance to compression depends on the quality factor that is pre-decided. Table 2 represents the results of applying varying levels of JPEG compression to the watermarked images and then authenticating them. The coefficients are quantized for 50% quality at the time of watermarking and are quite robust to Jpeg compression above 50%. The efficiency of the algorithm in extraction of the watermark can be given by the percentage difference computed between the calculated and extracted watermark. Percentage of up to 12-13% can be considered as acceptable.

Table 2: Authentication of watermarked images after JPEG compression

Jpeg= 90%	Jpeg=80%	Jpeg=75%	Jpeg=60%
(a) 3%	(b) 5%	(c) 7%	(d) 11%
(e) 4%	(f) 5%	(g) 6%	(h) 13%
(i) 3%	(j) 7%	(k) 8%	(l) 11%
(m) 2%	(n) 6%	(o) 8%	(p) 10%
			

3.3 Tolerance to Incidental attacks

Images are subject to incidental noise during storage and transmission. This noise introduces mild noise to the entire image but the distortion does not introduce semantic modifications. The watermarked image is subject to common incidental noises as mentioned in Table 4. The extracted and calculated watermarks are compared and evaluated in terms of the highest percentage difference observed between them. The results demonstrate that the watermark is highly tolerant to Gaussian noise and median filtering and is sensitive towards histogram equalization operations.

Table 3: Authentication results after incidental mild noise

Attack	Lena – Grey Scale	
	Attack	**Highest % Difference**

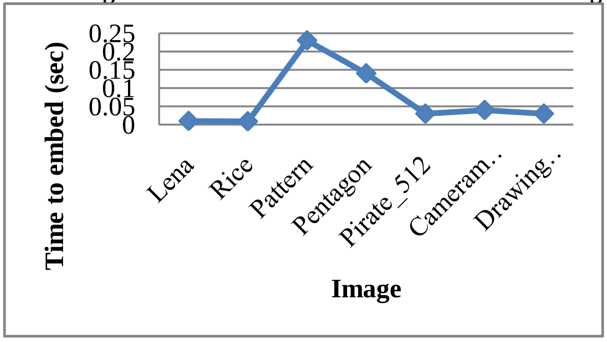
Gaussian Noise
M=0
V=0.01
		0%

Salt & Pepper Noise 0.01		0.19%
Histogram equalization 0 - 200		9%
Median Filter 3x3		0%

3.4 Time complexity

The time taken to generate the PQ sequence, generating the watermark and embedding is quite appreciable from Figure 3.

Figure 3: Time measure for watermark generation, scrambling and embedding



4. CONCLUSION

A semi fragile watermarking algorithm to authenticate images that may be JPEG compressed up to a certain quality factor. The feature vector is derived from the relationship between the corresponding DC and selected AC coefficients of each pair of blocks of the image and are used to embed the difference of selected DCT coefficients in the mid frequency domain so as to not cause visible distortions. The coefficients to be embedded are also determined randomly. The PSNR of the original and watermarked image is more than 50 dB which indicates good quality of the watermarked images. This scheme can be used in artistic, military and medical applications where it is necessary to ensure the originality and quality of the image after watermarking. The scheme is robust to Jpeg compression and mild incidental noise.

5. REFERENCES

[1] F. Namazi, M. R. Karami, and S. B. Ramazannia, “Block-based Adaptive Image Watermarking Scheme using Visual Perception Model in DCT Domain,” *Int. J. Comput. Appl.*, vol. 41, no. 4, pp. 41–45, Mar. 2012.

[2] F. Zhang, W. Liu, W. Lin, S. Member, and K. N. Ngan, “Spread Spectrum Image Watermarking Based on Perceptual Quality Metric,” *IEEE Trans. IMAGE Process.*, vol. 20, no. 11, pp. 3207–3218, 2011.

[3] N. Memon, P. W. Wong, and S. Member, “A Buyer – Seller Watermarking Protocol,” *IEEE Trans. IMAGE Process.*, vol. 10, no. 4, pp. 643–649, 2001.

[4] C. I. Podilchuk and E. J. Delp, “Digital WM : Algoritms and applications,” *IEEE Signal Process. Mag.*, no. July, pp. 33–46, 2001.

[5] R. S. Alomari and A. Al-jaber, “A Fragile Watermarking Algorithm for Content Authentication,” *Int. J. Comput. Inf. Sci. Vol.2,*, vol. 2, no. 1, pp. 27–37, 2004.

[6] S. Garg, “An Efficient Method for Digital Image Watermarking Based on PN Sequences,” *Int. J. Comput. Sci. Eng.*, vol. 4, no. 09, pp. 1550–1561, 2012.

[7] A. Masmoudi, M. S. Bouhlel, and W. Puech, “A New Image Cryptosystem based on Cahotic Map and Continued Fractions,” pp. 1504–1508, 2010.

[8] A. Masmoudi, “An Efficient PRBG Based on Chaotic Map and Engel Continued Fractions,” *J. Softw. Eng. Appl.*, vol. 03, no. 12, pp. 1141–1147, 2010.

[9] A. M. Kane, “On the Use of Continued Fractions for Mutual Authentication,” *Int. J. Inf. Secur. Sci.*, vol. 1, no. 3, 1995.

[10] A.M. Kane, “On the use of continued fractions for electronic cash,” *Int. J. Comput. Sci. Secur.*, no. 4, pp. 136–148, 2013

[11] Lin and S. Chang, “Generating Robust Digital Signature for Image / Video Authentication,” Multimedia and Security Workshop at ACM Multimedia ’98, Bristol, U.K., September, 1998.

[12] M. F. M. Mursi, G. M. R. Assassa, H. A. Aboalsamh, and K. Alghathbar, “A DCT-Based Secure JPEG Image Authentication Scheme,”, World Academy of Science, Engineering and Technology, vol 3, pp. 611–616, 2009.

[13] C. Chang, J. Chuang, and T. Chen, “Recognition of Image Authenticity Using Significant DCT Coefficients Quantization,” Informatica, vol. 26, pp. 359–366, 2002.

[14] Van Schyndel, R.G., Tirkel, A.Z. and Osborne, C.F., 1994. “A digital watermark”, Proceedings of IEEE International Conference on Image Processing, Vol. 2, pp. 86-90.

[15] Mitr, A., “On Pseudo-Random and Orthogonal Binary Spreading Sequences”, International Journal of Information and Communication Engineering. 2008.

[16] H. Niederreiter, Sequences with almost perfect linear complexity profile, Advances in Cryptology - EUROCRYPT’ 87: Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, vol. 304, 37-51, 198

[17] C. D. Olds, “Continued Fractions”, Random House, 1963.

[18] O. Perron, “Die Lehre Von Den Kettenbrüchen”, 3rd ed. (1954)

[19] A. M. Kane, “On the use of Continued Fractions for Stream Ciphers” In Proceedings of Security and Management 2009, Las Vegas, USA.

[20] A. G. B. Lauder, Continued fractions and sequences, Ph.D. thesis, University of London, 1999.

[21] J. Pieprzyk, H. Ghodosi, C. Charnes, R. Safavi-Naini Cryptography based on transcendental numbers, Information Security and Privacy, Lecture Notes in Computer Science, Vol. 1172, Proceedings, First Australasian Conference on Information Security and Privacy, ACISP’96,Wollongong, Australia, 1996.

[22] C. Shine, Method and apparatus of using irrational numbers in random number generators for cryptography United States Patent, Application No. 10/190455, Application Date: Jul 3 2002.

[23] P. Jayashree, T. Padma, “Image Watermarking using PQ sequences”, Proceedings of the International Conference on Emerging Research in Computing, Information, Communication and Applications (Vol 3) Elsevier Publications 2014, ISBN 9789351072638

[24] Parthasarathy, Arvind Kumar, Kak, Subhash, “An Improved Method of Content Based Image Watermarking,” , IEEE Transactions on Broadcasting, vol. 53, no. 2, pp. 468–479, 2007.

[25] S. Garg, “An Efficient Method for Digital Image Watermarking Based on PN Sequences,” *Int. J. Comput. Sci. Eng.*, vol. 4, no. 09, pp. 1550–1561, 2012

[26] Jayashree S. Pillai, T. Padma, The analysis of PQ sequences generated from continued fraction for use as pseudorandom sequences in Cryptographic Applications, *Springer AISC Series, 2015.*