Article can be accessed online at http://www.publishingindia.com

Secure Watermarking using Diophantine Equations for Authentication and Recovery

Jayashree Nair*, T. Padma**

Abstract

This paper describes an authentication scheme that uses Diophantine equations based generation of the secret locations to embed the authentication and recovery watermark in the DWT sub-bands. The security lies in the difficulty of finding a solution to the Diophantine equation. The scheme uses the content invariant features of the image as a self-authenticating watermark and a quantized down sampled approximation of the original image as a recovery watermark for visual authentication, both embedded securely using secret locations generated from solution of the Diophantine equations formed from the PQ sequences. The scheme is mildly robust to Jpeg compression and highly robust to Jpeg2000 compression. The scheme also ensures highly imperceptible watermarked images as the spatio – frequency properties of DWT are utilized to embed the dual watermarks.

Keywords: Diophantine Equations, Content authentication, Authentication Watermark, Recovery Watermark, PQ Vector, DWT

Introduction

Image authentication is the process of verifying and validating the integrity of the watermarked data. It is also the act of confirming if the image is credible or not. In any authentication system, imperceptibility of the watermark, fragility to detect tampering, security to ensure difficulty to tamper with the image and watermark and efficient computation are the desirable characteristics.

In this paper, the prospect of using Diophantine equations in facilitating a secure watermark embedding, verification, and recovery scheme for image authentication is explored.

Diophantine Equations

A Diophantine equation (Menezes, van Oorschot, & Vanstone, 1997; Yosh, 2011) is an algebraic equation, usually in two or more unknowns, such that only integer solutions are sought or allowed. The word *Diophantine* refers to the Hellenistic mathematician of the 3rd century, Diophantus of Alexandria, who made a study of such equations and was one of the first mathematicians to introduce symbolism into algebra.

Diophantine Equations are polynomial equations of the form

$$f(a_1, a_2, a_3, \ldots a_n, x_1, x_2, x_3, \ldots \ldots x_n) = C \qquad (1)$$

where and C are integers. The simplest of the equations are the linear equations of the form

$$ax_1 + bx_2 = C \qquad (2)$$

In spite of many efforts to find a general algorithm, finding solutions to Diophantine equations is usually a hard task and individual equations present a kind of puzzle and have been considered throughout history. This is because of the fact that the Diophantine equation may have zero non-trivial solution, finite number or infinite number of solutions and there is no polynomial time solution to finding the solvability of the equation. This property has been used by many researchers to define cryptosystems (Laih 1997; Schnorr, 1995; Lin, Chang, & Lee, 1995).

* Associate Professor, Acharya Institute of Management & Sciences, Peenya, Bangalore, Karnataka, India. Email: nair.jayashree@gmail.com

** Professor, Sona College of Engineering, Salem, Tamil Nadu, India. Email - padmatheagarajan@gmail.com

Lin *et al.* (1995) proposed a public key cipher scheme based on Diophantine equations.

Yosh (2011) proposed key exchange cryptosystem where two higher order Diophantine equations are considered for encrypting shared secret between sender and recipient. The senders and recipient exchange Diophantine equations as their public key. Although this key exchange cryptosystem has the intrinsic security, it requires a complicated implementation compared with other key exchange cryptosystems. This complexity is due to generating Diophantine equations in an unpredictable manner so as to avoid cases of generating equations that have unique solutions.

Hirata-Kohno, & Petho (2013) analysed the protocol due to Yosh (2011), revealing several weaknesses of the protocol, and suggested a modification of it. They removed partially the weaknesses and suggested a choice of the parameters, which is secure against cipher text-only attack.

Attila, Lajos, & Noriko (2014) proposed a key exchange protocol relying on the hardness of solving Diophantine equations proposed by Yosh (2011) and combined it with the complexity of S-integers, where the public key size is much less but provides same level of security.

The Proposed Scheme

In this scheme, two watermarks are generated – the authentication watermark W_A and recovery watermark W_R. W_A is used to detect incidental or malicious tampering and is embedded in the HL_1 sub band. W_R is the quantized approximation of the original image and is used for visual authentication. is embedded into the least significant bits (LSB) of the coefficients of the LH_1 suband. In order to enhance the security of the watermarking scheme, Diophantine equations are generated at the senders side, whose selected solutions are used to identify embedding locations for the watermarks W_A and W_R. The receivers' side authenticates the watermarked image after regenerating the solutions to the Diophantine equations and identifying the embedding locations of the watermarks. The watermarking scheme is explained in 4 phases: 1) Generation of the PQ Vector and Diophantine equation, 2) Generation and embedding of the authentication watermark, 3) Generation and embedding of the recovery watermark, and 4) Image authentication and verification.

Generation of the PQ Vector PQV and Diophantine Equation

The PQ sequences generated from the partial quotients of the continued fraction expansions of certain irrational numbers have previously been analysed by the authors for pseudo randomness in Attila *et al.* (2014). In order to enhance the pseudo randomness of the sequence, multiple sequences are extracted from locations $L1$ and $L2$ of the PQ sequence and XORed to generate the PQ Vector PQR. The locations $L1$ and $L2$ are so chosen so as to form a Diophantine equation of the form

$$Ax_1 + bx_2 = C \tag{3}$$

$$L1x_1 + L2x_2 = C \tag{4}$$

where $a = L1$, $b =$ L2, and C are secret integers and

L1, L2 and C are integers with not both L1 and L2 not equal to 0 and if g = *gcd* ($L1$, $L2$) then g/c as the Diophantine equation will have infinitely many solutions.

The Diophantine equation generated is solved for the basic solution. The pth solution for x_1 and x_2 is selected as the start of the prospective secret embedding locations, for embedding the authentication watermark W_A and EL2 for embedding the recovery watermark W_R where

$EL1 = x_1 \bmod n$

and $EL2 = x_2 \bmod n$ (5)

where n is the number of coefficients in the sub band.

Generation and Embedding of Authentication Watermark W_A

Generation of W_A

The 1st level DWT transform of the host image decomposes the image into 4 sub bands – LL_1, LH_1, HL_1 and HH_1. The DCT of the LL_1 sub band is considered to generate the feature vector FV using the technique proposed in Lin & Chang (2001). This feature vector is scrambled using the PQ Vector *PQV*, generated from the PQ sequence in "The analysis of PQ sequences" (n.d.) to w generate the authentication atermark W_A. Multiple copies of the scrambled feature vector in embedded into the horizontal and vertical sub bands obtained after further DWT decomposition of the HL_1 sub band.

Embedding of W_A

The generated watermark is embedded into the horizontal and vertical detail sub bands as follows:

1. Apply DWT to the *HL*1 sub band to obtain the sub bands as in Fig. 2(b). The *HHL*2 and *HLH*2 sub-bands are considered for embedding the watermark bits.
2. Vectors *V*1 and *V*2 are formed of *HHL*2 and *HLH*2 sub-bands starting with positions *EL*1 obtained as shown in previous section.
3. Evaluate the ratio of the coefficients at the corresponding positions

   $$R(i) = (sgn)\, V1(i)/V2(i) \quad (6)$$

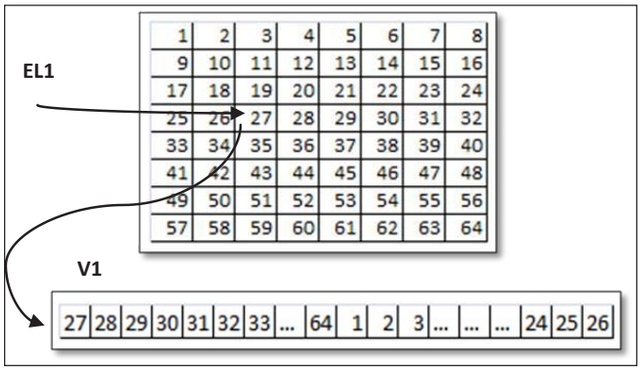
   This vector will be the side information to be shared with the authenticator in a secure manner.
4. Modify the amplitude of the corresponding coefficients of *V*1 and *V*2 vectors to embed the watermark:

   $$if M_b = 1, \quad \begin{cases} V1 = V1 * \alpha \\ \quad and \\ V2 = V2/\alpha \end{cases} \quad (7)$$

   $$if M_b = 0, \quad \begin{cases} V1 = V1/\alpha \\ \quad and \\ V2 = V2 * \alpha \end{cases} \quad (8)$$

where α is the watermark strength factor and can be experimentally determined. It has a value larger than one and α = 1.2 gives good imperceptibility in the experiments conducted. The ratio R' (i) after embedding M_b will increase if M_b = 1 and decrease if M_b = 0.

Fig 1: Vector *V*1 formed of the *HHL*2 Sub Band Starting with Position Referenced by



Generation and Embedding of Recovery Watermark W_R

Generation of W_R

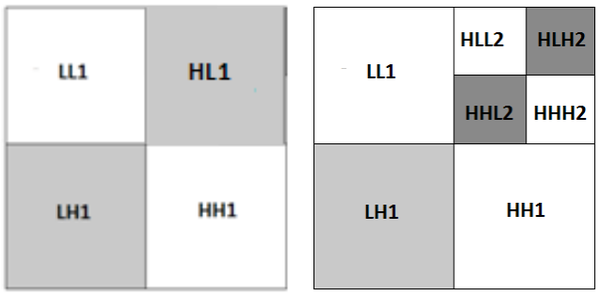
The recovery watermark is generated by further 2 level DWT decomposition of the *LL*1 sub-band to obtain a coarse representation *LL*3. The coefficients of *LL*3 sub-band are then suitably quantized using Quantized Index Modulation Chen & Wornell (1998) to decrease the obtrusiveness of the coefficients and represent it uniformly.

Embedding of W_R

The quantized coefficients are embedded by replacing 5 least significant bits of the coefficients of the LH1 sub-band, starting from the position selected based on the pth solution of the Diophantine equation for *EL*2 as specified in previous section.

Apply inverse DWT to get the watermarked image W_m

Fig. 2: (a) and (b) Embedding Locations of the Authentication and Recovery Watermarks

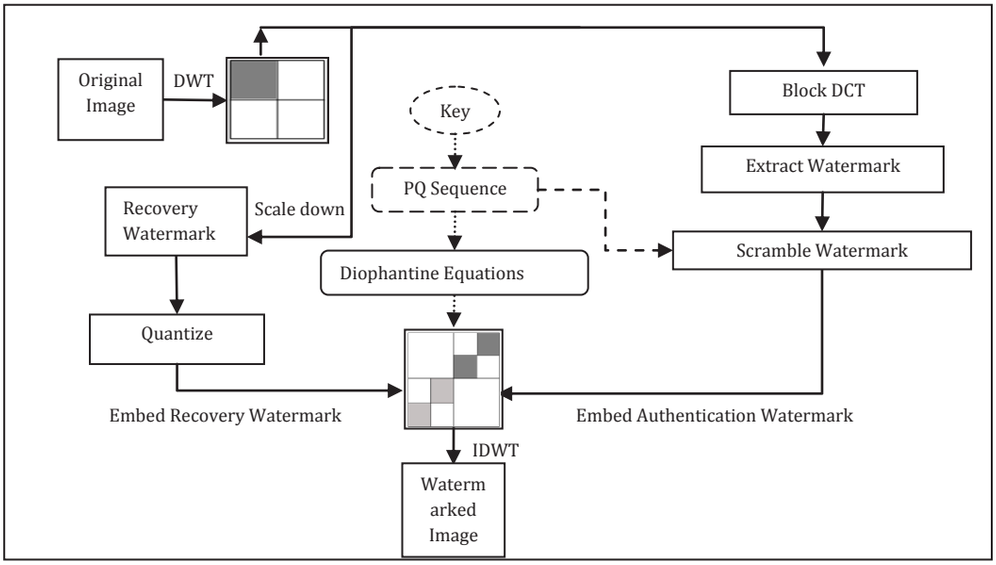


(a) (b)

Extraction of the Authentication Watermark and Verification of Integrity

The watermark extraction procedure is similar to the watermark generation and insertion procedure. The vector R should be made available at the authenticating end which can be shared using a secret key or public key system or kept in the repository secured by means of Public Key Infrastructure (PKI). The PQ sequence and PQ Vector *PQV* is regenerated at the authenticator. The watermark extraction steps can be explained as follows:

Fig. 3: Overall Scheme for Generation of Authentication and Recovery Watermark



Generation of the Authentication Watermark

Applying the procedure in earlier section "Generation of W_A", the authentication watermark W_A^* is generated from the watermarked image W_m.

Extraction of the Embedded Authentication Watermark

1. Applying Step 1, 2 and 3 of the procedure in section "Embedding of W_A",

$$R^{\sim}(i,j) = (sign)\left(\frac{HHL2^{\sim}(i,j)}{HLH2^{\sim}(i,j)}\right) \quad (8)$$

is evaluated for the watermarked image.

2. Extract the Majority bit using the relationship

$$M_b^{\sim} = \begin{cases} 1 & if\ {}^{R^{\sim}}/_{R} > 0 \\ 0 & otherwise \end{cases} \quad (9)$$

3. The string of is the extracted watermark. Compare the generated watermark and the extracted watermark to authenticate the image and verify the integrity. If the integrity is verified, then the watermarked image can be reversed back to the original image.

Extraction of the Recovery Watermark

To extract the estimated image, the reverse procedure of the recovery watermark generation and embedding is performed. The corresponding sub-band is selected and 5 least significant bits from the coefficients, positions identified by EL2~, are extracted. The extracted bits are used to reconstruct the quantized coefficient values and recovery watermark

Performance Evaluation

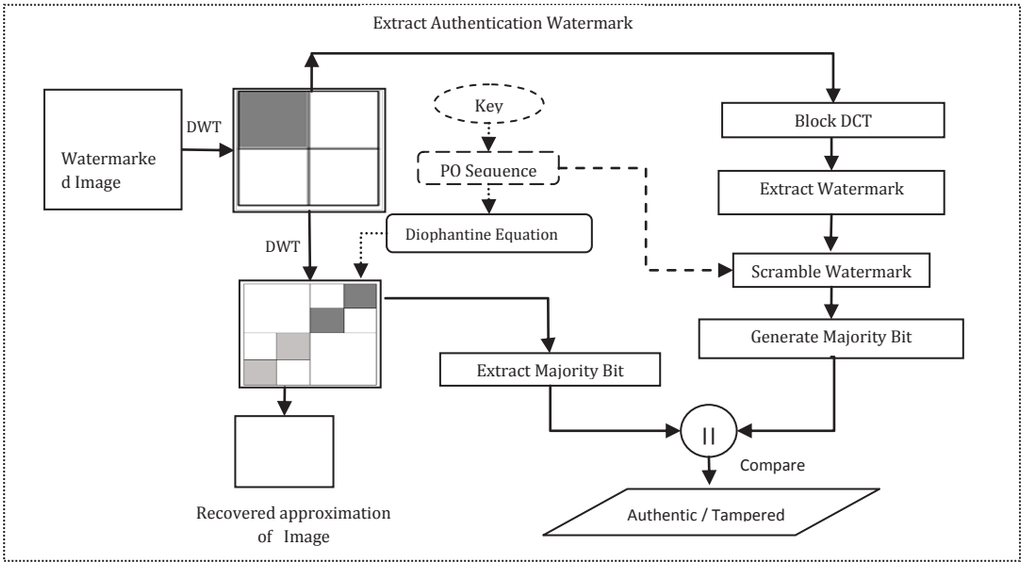
The scheme described in this paper is implemented in Matlab environment. Images of type tiff, bmp, png, and colour images of various sizes and complexities were considered for the simulation.

The choice of embedding the authentication watermark W_A or recovery watermark W_R or both can be decided based on the requirement of the application. The embedding of the recovery watermark reduces the quality of the watermark but is still above acceptable limits.

Imperceptibility Analysis

The quality of the watermarked images after embedding the $W_A$only and both W_A and W_R is summarised in Table 1. The Peak Signal to Noise Ratio (PSNR) of the images watermarked with only W_A are in the range 51- 62 and after embedding both W_A and W_R are in the range 39 – 42dB. A PSNR

Fig. 4: Overall Scheme for Verification and Recovery



of 30dB and above indicates good quality of the watermarked image.

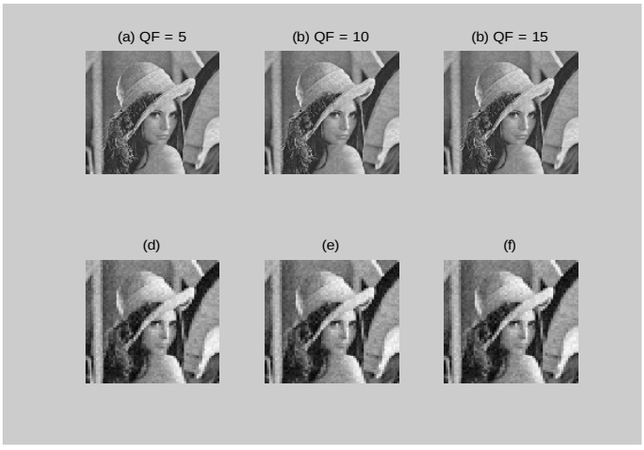
The Mean Square Error (MSE) of the watermarked images varies between 0.03 and 0.5 for only W_A and between 7.1 and 9.2 for both W_A and W_R. Structural Similarity (SSIM) which is a measure of the similarity between the compared images is in the range of 0.96 to 0.99, which indicated that the original and watermarked images are very similar. For both W_A and W_R the values are in the range 0.93 to 0.98. The Pearson Correlation Coefficient (PCC) also gives a measure of the correlation between the compared images and has a value 1 for only W_A and 0.99 for both W_A and W_R.

Tolerance to Compression

JPEG Compression

Any image authentication system should be robust to compression attacks. The robustness of the scheme is evaluated by compressing the watermarked image with different quality indices and then trying to extract the image. The results in Table 2 and Fig. 4 indicate the scheme is robust to JPEG2000 compression with quality factor up to 20 which is the highest permissible value in JPEG2000 compression. JPEG2000 is the current compression standard used for images even through it adoption is progressing slowly.

Fig.5 (a), (b) and (c) : Lena Watermarked Images After Jpeg 2000 Compression with Quality Factor (QF) 5, 10 and 15 (d), (e) and (f): The Corresponding Recovered Image After the Compression



Even though JPEG 2000 is the current standard for image compression, it will take some time before it is universally implemented. Till such time, JPEG compression will be prevalent. The results in Fig. 5 and Table 2 indicate the scheme is not very robust to JPEG compression beyond 85%. Fig. (d), (e) and (f) show the recovery watermark extracted from the JPEG compressed image

Table 1: Quality of the Watermarked Images with Single and Dual Watermarking

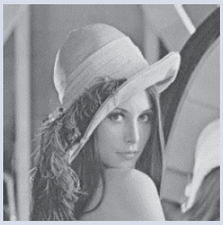
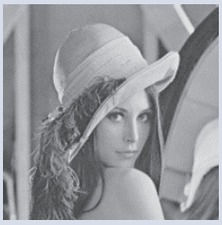
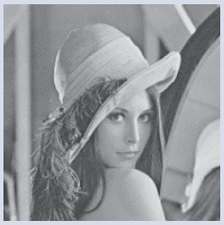
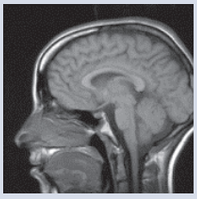
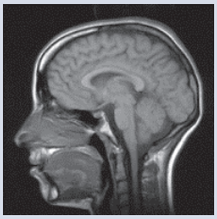
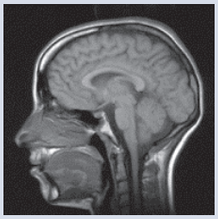
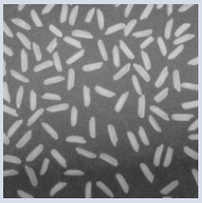
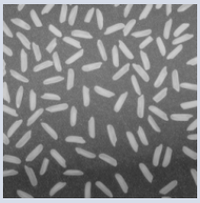
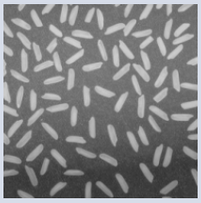
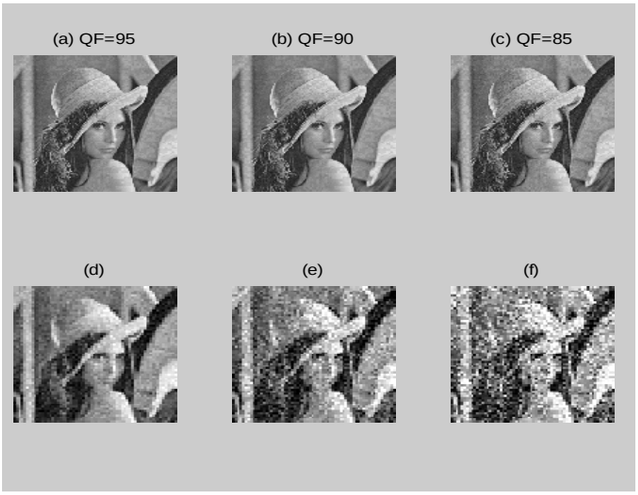
Original Image	*Image with Authentication Watermark*	*Image with Authentication and Recovery Watermark*
		
PSNR MSE SSIM PCC	62.85dB 0.033 0.99 1	40dB 7.1 0.942 0.998
		
PSNR MSE SSIM PCC	61.68 dB 0.04 1 1	42.7 dB 3.51 0.983 0.999
		
PSNR MSE SSIM PCC	60.15 dB 0.06 0.99 1	41 dB 8.10 0.93 0.995
		
PSNR MSE SSIM PCC	51.01 dB 0.51 0.96 1	39 dB 9.24 0.93 0.992

Fig 6 (a), (b) and (c) : Lena Watermarked Images after JPEG Compression with Quality Factor (QF) 95, 90 and 85 (d), (e) and (f) : The Corresponding Recovered Image After the Compression



Tolerance to Noise

Addition of noise is one method of estimation of robustness of the watermark. Noise distorts and degrades the image which in turn distorts the content based watermark.

Table 2: Performance of the Semi Fragile Authentication Results Under Various Attacks for Watermarked Image of Lena. Correlation and PSNR are Calculated for the Recovered Watermark After the Attack. Percent of Tampered Blocks is the Output of the Authenticator

Attacks	*Authentication Results*	*Recovery Results*	
	Percentage of blocks detected as tampered	*Correlation value*	*PSNR value*
Original water-marked image	Nil	1	65
Wrong key	78%	-	-
Jpeg 95%	10%	0.97	42.92
Jpeg 90%	28%	0.93	38
Jpeg2000 QF=5	2%	1	55.3
Jpeg2000 QF=10	5%	1	53.6
Jpeg2000 QF=15	9%	1	50.4
Jpeg2000 QF=20	10%	1	50
Median Filter [3 3]	40%	0.3	13
Median Filter [4 4]	36%	0.4	17
Gaussian blur M=0; V=0.001	8%	0.87	31
Salt and pepper Noise density =0.02	16%	0.53	21
Salt and pepper Noise density =0.01	12%	0.82	30
Non water-marked image	70%	-0.03	9

Security Analysis

Randomness of the PQ Sequence

The authentication system is as secure as the randomness of the pseudorandom sequences used to scramble the watermark or its embedding sequence. The randomness of the PQ sequences has been established previously in "The analysis of PQ sequences" (n.d.).

Randomness in Selection of the Embedding Locations

Locations to embed the watermark in the images are usually pre-determined so as to enable its retrieval at the authentication end. Very often pseudorandom sequences are also used to identify the embedding locations. In order to enhance the security of the scheme and make it even more difficult for the adversary, Diophantine equations are used to generate the identifying locations. The difficulty in solving the equations is used to add to the security. Hence in a 128*128 sub-band having 16,384 coefficients, the adversary has to a) either try all possible locations for the presence of the watermark or has to solve the Diophantine equation knowing the secret values of L1, L2 and C or the pth solution of the equation. This makes the complexity quite high.

Conclusion

This paper describes an authentication scheme that uses Diophantine equations based generation of the secret locations to embed the authentication and recovery watermark in the DWT sub-bands. The security lies in the difficulty of finding a solution to the Diophantine equation. The scheme uses the content invariant features of the image as a self authenticating watermark and a quantized down sampled approximation of the original image as a recovery watermark for visual authentication, both embedded securely using secret locations generated from solution of the Diophantine equations formed from the PQ sequences. The scheme is mildly robust to Jpeg compression and highly robust to Jpeg2000 compression. The scheme also ensures highly imperceptible watermarked images as the spatio – frequency properties of DWT are utilized to embed the dual watermarks.

References

Attila, B., Lajos, H., & Noriko, H, (2014). *A key exchange protocol based on Diophantine equations and S-integers*. JSIAM Letters, 6, 85-88, Japan Society for Industrial and Applied Mathematics.

Chen, B., & Wornell, G.W. (1998). *Digital watermarking and information embedding using dither modulation*. Proceedings of the IEEE workshop on Multimedia Signal Processing (MMSP-98), Redondo Beach, CA, December.

Chuang, J. C. et.al., (2013). Grayscale image tamper detection and recovery based on vector quantization. *International Journal of Security and its Applications*, 7(6), 209-228.

Hirata-Kohno, N., & Petho, A. (2013). *On a key exchange protocol based on Diophantine equations*. *Infocommunications Journal*, 5(3), 17-21.

Hu, Y. C., Lo, C. C., Chen, W. L., & Wen, C. H. (2013). Joint image coding and image authentication based on AMBTC. *Journal of Electronic Imaging*, 22(1), (1-12).

Kane, A. M. (1995). On the use of continued fractions for mutual authentication. *International Journal of Information Security Science*, 1(3), 88-99.

Kane, A. M. (2013). On the use of continued fractions for electronic cash. *International Journal of Computer Science and Security*, 4(1), 136-148.

Kundur, D., & Hatzinakos, D. (1999). *Digital watermarking for telltale tamper proofing and authentication*. Proceedings of the IEEE, 87(7), 1167-1180.

Laih, C. S. (1997). *Cryptanalysis of Diophantine equation oriented public key cryptosystem.* IEEE Transactions on Computers, April, 46(4), 399-411.

Lie, W. N., Lin, G. S., & Chen, S. L. (2006). *Dual protection of JPEG images based on informed embedding and two-stage watermark extraction techniques*. IEEE Transactions on Information Forensics and Security, 1 (3), 330-341.

Lin, C. Y., & Chang, S.F. (2001). *SARI: Self-authentication-and-recovery image watermarking system*. ACM Multimedia, Ottawa, Canada: ACM Press. (pp.628-629).

Lin, C. H., Chang, C. C., & Lee, R. C. T. (1995). *A new public-key cipher system based upon the Diophantine equations.* IEEE Transactions on Computers, 44(1), 13-19.

Lin, C. Y., & Chang, S. F. (2001). *A robust image authentication method distinguish JPEG compression from malicious manipulation*. IEEE Transactions on Circuits and Systems of Video Technology, 11(2), 153-168.

Lu, C. S., & Laio, H. Y. M. (2001). *Multipurpose watermarking for image authentication and protection*. IEEE Transactions on Image Processing, 10(10), 435-439.

Masmoudi, A., Bouhlel, M. S., & Puech, W. (2010). *A new image cryptosystem based on chaotic map and continued fractions*. 18th European Signal Processing Conference (EUSIPCO-2010), (pp. 1504-1508).

Masmoudi, A. (2010). An efficient PRBG based on chaotic map and Engel continued fractions. *Journal of Software Engineering and Applications*, 3(12), 1141-1147.

Menezes, A. J., vanOorschot, P. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*. CRC Press Series on Discrete Mathematics and its Applications. Boca Raton, FL.

Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). *An Introduction to the Theory of Numbers* (5thEd), John Wiley $\ & $ Sons, New York.

Ong, H., Schnorr, C., & Shamir, A. (1985). *An efficient signature scheme based on polynomial equations.* Proceedings of CRYPTO, (pp 37-46).

Patra, J. C., Phua, J. E., & Bornand, C. (2010). A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. *Digital Signal Processing*, 20(6), 1597-1611.

Qi, X., & Xin, X. (2011). A quantization-based semi-fragile watermarking scheme for image content authentication. *Journal of Visual Communication and Image Representation*, 22(2), 187-200.

Seng, W. C. (2009). Semi fragile watermark with self authentication and self recovery. *Malaysian Journal of Computer Science*, 22(1), 64-84

The analysis of PQ sequences generated from continued fraction for use as pseudorandom sequences in Cryptographic Applications, Springer AISC Series, August 2015.

Yosh, H. (2011). The key exchange cryptosystem used with higher order Diophantine equations. *International Journal of Network Security & Its Applications*, 3(2), 43-50.