ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

Information Security and Sender's Rights Protection through Embedded Public Key Signature

Vineeta Khemchandani[1], Prof G.N.Purohit[2]

[1] Department of Computer Applications, JSS Academy of Technical Education
NOIDA, Uttar Pradesh, 201301, India

[2] AIM & ACT, Banasthali University
P.O, Banasthali Vidyapith, Rajasthan, 304022, India

Abstract

Information security is not just to provide an authenticity and integrity to the data, but there is also a need to seek identity, rights of use and origin of information, which may require some degree of process re-engineering. Rarely security technologies like digital signatures can be simply "plugged in" without streamlining the process. In this paper we address the problem of information security and protecting the rights of originator of the structured document from ill-intentioned recipient who can modify the received decrypted information. At sender end, a public key signature is generated using SHA-1 or SHA-2. Signature is embedded into raster image of the document using non-invertible robust public key watermarking technique based on orthogonal signals concepts. The document is then encrypted with public key of the receiver using RSA algorithm to achieve confidentiality and authorization. The proposed scheme uses correlation analysis to detect embedded signature to authenticate message. This scheme also uses Gauss-Jordan method to derive the signature from the watermarked image to verify ownership. The study is corroborated with result and application of the proposed technique to prevent forgery and alteration in e-cheque document.

***Keywords**: Digital Signature, watermarking, Information Security, Rights Protection, cheque alteration, signature forgery.*

1 Introduction

Over the past few years there has been tremendous growth in computer networks especially in the field of World Wide Web. This phenomenon coupled with the exponential increase of computer performance, has facilitated on-line business operations like shopping, trading, cheque truncation, bill presentment. Due to massive use of personal computers, network and the Internet, new features of security are in need. In addition to confidentiality, authentication, integrity and control, one must think of new security requirements like protecting the rights of originator against tampering and illegal distribution of the information by the intended recipient, as an ill intentioned authorized recipient can modify and redistribute the decrypted information.

It is well known that cryptography deals with unauthorized access but there are functional limitations like requirement of global clock synchronization, handshaking and costly tamper proof hardware. Digital watermarking is a technique based on digital signal processing which inserts extra signal to digital contents for discouraging illicit modification and distribution of information and to authenticate watermarked contents. But, digital watermarking has the following limitations: -

(a) No transmission security – due to lack of public key algorithms.
(b)Text information - Due to binary block format of the text, embedding new bits in the text may introduce irregularities that are visually noticeable.

This paper presents a technique, which contains strengths of digital signature and digital watermarking both so as to provide a secure transmission of messages. Thus the rights of sender on digital content are protected. Figure 1 illustrates an approach that uses raster representation of the document in which digital signature is embedded as watermark. Public key signature protects the document from any intruder, while embedding it as resilient, non-invertible and robust watermark prevents non-trusted receiver to modify the contents of the document.

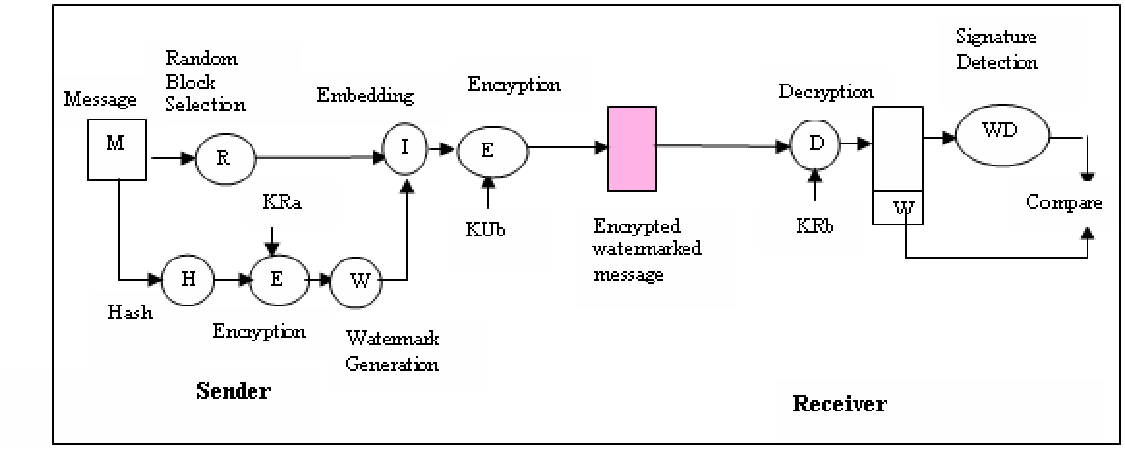


Figure 1 Public Key Cryptosystem with embedded digital signature

The rest of the paper is organized as follows. Section 2 presents digital signatures and watermarking, section 3 describes digital signature generation and embedding procedures, section 4 contains detection of watermark to prove authenticity, and section 5 contains verification of watermark to prove ownership, experimental results are then discussed in section 6 for the purpose of performance evaluation. Conclusion will be given in section 7.

2 Digital Signatures and Watermarking

The ownership protection, authentication and integrity of structured document is necessary and important. Encryption and digital signature techniques protect against eavesdroppers, for sure, but the main attacks are likely to be from validly connected end-users who go on to redistribute the received data more than they are entitled to. Digital signature uses “Public-Key Cryptography” which employs an algorithm using two different but mathematically related “keys” one for creating signature, and, another for verifying signature. Compare this to information hiding the cryptographic signature is embedded into the information itself. Watermarking [1] is a security technique in context of protecting content of information from authorized user. It is as old as paper production is and protects rights of author/originator. This technique is basically used to identify any processing and modification in the contents.

2.1 Digital Signatures

Digital signatures have been accepted in several national and international corporations, banks and government agencies. The fundamental process involved in digital signature is a hash function. A number of hash functions are proposed in the literature. The MD5 message digest algorithm,[2] was developed by Ren Rivest at MIT. MD5 generates a 128 bits message digest out of a variable length message. Another hash algorithm SHA (Secure Hash Algorithm) was developed by National Institute of Standards and Technology (NIST) and published as a federal information processing standard [3] in 1993.Revised version of SHA is implemented in C language and referred as SHA-1 [4]. It generates 160 bits message digest. SHA-1 has achieved level of Standard because it generates 32 bits longer message digest than MD5, using a brute force technique for a given digest the difficulty in achieving message is of the order of 2^{160} operations in comparison to 2^{128} operations in MD5.In the draft FIPS 180-2 NIST published SHA-2 as a new version of secure hash algorithm. SHA-2 offers, SHA-1, SHA-256, SHA-384 and SHA-512. In other words SHA-2 may have outputs160, 256, 384, and 512 bits of message digest. However, SHA-2 algorithm uses fixed and predefined parameters that may be vulnerable to attack.

Digital signature can save the message from third parties [5] but once an encrypted message is at receiver end, an ill-intentioned receiver can easily decrypt, modify and distribute the message for commercial benefits. This means the sensitive information in these messages cannot be protected from modification and redistribution from the authorized receiver using encryption, access restriction and hiding information behind firewalls.

2.2 Digital Watermarking

A digital watermark is a distinguished piece of information that is adhered to the data that it is intended to protect. Several embedding techniques [1, 6-8] have been specially developed for use with text but most of these techniques either change word or line spacing or make change on the character boundary which require original document to detect watermark to authenticate sender. These techniques cannot be simply used to embed digital signature due to involvement of integrity issues with digital signature applications.

Tao Chen, et al suggests a combined digital signature and digital watermarking scheme [9] for image authentication and content protection. In this scheme content dependent random k bits are extracted from N blocks of image to obtained K X N bits signature, which is embedded back to the image using secret key. Due to requirement of large number of keys this method cannot be used in applications requiring transmission of data.

Ding Huang presents a text watermarking technique [10] that expands and shrinks widths between words to represent inter word distance, as sine wave. In this method sine wave is coded as watermark. This technique cannot be used to send confidential message, as it does not use any key.

Chang & Chang presented a sender-buyer protocol [11] where digital signature containing sender, buyer and trading information is embedded in the image as barcode image. This scheme protects the embedded trading message and ensures integrity of image but does not authenticate the sender, as digital signature is not based on content of the information.

Cor et al [12] proposed secure spread spectrum watermarking scheme. A two-dimensional spectrum signal is generated. 128 low bits of the spectrum signal are modulated with 128 bits of the owner's secret key. Adding modulated signal back to the image generates the watermark signal. Inverting spectrum signal, which is then added to the image, generates watermark signal. Drawbacks of this scheme are (1) it requires original image to detect the watermark and (2) Every time new binary key is needed to protect new image.

Natrajan presented a paper for watermarking of digital images to detect or verify ownership [13]. In this method most common RSA & DSS public key signature generation algorithms are used to generate public and private keys of user. This method involves computing message digest using MD5 of image I of M rows and N columns. Message digest is encrypted with private key to generate digital signature. Low order bits of DS are modulated to as watermark and inserted back into the image.

We can summaries that, in order to protect document integrity and rights of owner on the document the crypto signature should be content based and public in order to avoid the large number of secret keys. Secondly such a scheme should not require original document to detect and verify the ownership and should be computationally inexpensive.

The goal of this work is to design a cipher model that contains strengths of digital signature and digital watermarking both to provide secure structured document transmission and to detect and verify ownership to prevent alteration and forgery. The approach uses raster representation of the document in which digital signature is embedded as watermark. Public key digital signature protects the document from third party while embedding it as watermark prevents non-trusted receiver to modify the contents of document.

3. Embedding Digital Signature

3.1 Image representation of a message

The process starts with calculating size of the text information and then converting it into its digital image representation. Input text is stored in string format before conversion. Size of the text is calculated in the form of an invisible drawing in the context of memory device. The height and width are calculated as shown in figure 2..

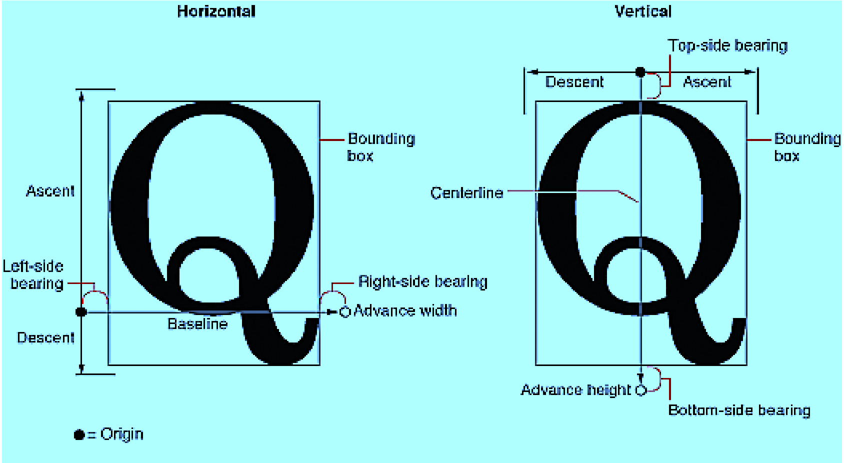


Figure 2: Image size Measurement

Image height = (Ascent+ Descent+ bearing) * No. of lines in text message (1)

Image width = = Max (x [i]); 0<= i <=no. of lines (2)

True color RGB model is used to represent image as a bit frame of size width*height, where, each square represents a value of bit as function f (x, y).

{f (x, y) = [0,1], | x= 0 to width, y = 0 to eight} . (3)

A total number of 32 frames for a single image are used [14]. The first 8 frames represent transparency; the next 24 frames (8 per color) are used to represent Red, Green and Blue colors respectively. The binary values (0 or 1) in corresponding bits from each of the 32 bit planes result in a binary number to represent pixel's intensity level from 0 to 2^{32} –1 (full intensity).

For each bit, in all 32 bit frames, value of function f(x, y) is set to 0 to create a white background image.

{f (x, y) = 0 | x= 0 to width, y = 0 to height} (4)

Value of function f (x, y) is manipulated at a specific location in all the bit frames to draw text pattern on the background image. Intensity of the image is set in all 32-bit frames to get a specific pixel value [15-17]. Values of pixels stored in memory are grabbed into a vector of size width * height.

3.2 Generation and Embedding of Digital signatures

This process starts with calculating a message digest from two-dimensional message signal M of m rows and n columns. One-way hash function H operates on input message M of arbitrary length and returns a fixed length hash value h, i.e. H (M) = h. It has additional characteristics as follows:

(i) Given M it is easy to compute h,
(ii) Given h it is hard to compute M / such that H (M $^{/}$) = h
(iii) Given M it is hard to compute another message M $^{/}$ such that H (M) = H (M $^{/}$).

Several methods are developed to find hash function [2-4]. Here SHA-I algorithm is used to generate unique 160 bits.

Then RSA algorithm is used to encrypt fixed length message digest using owner's private key to generate owner's public key signature vector [5]. Since RSA algorithm is based on the fact that there is insufficient way to factorize very large number, deducing the RSA key, therefore, requires very high computer processing time. RSA algorithm has also become de facto standard for industrial strength and built into many of the software products like Netscape Navigator and Internet Explorer.

Next, the bits of digital signature are modulated and transformed to compute watermark signal. Length of the watermark signal may be same as that of digital signature or it may be based on first, middle or last bits of the digital signature as long as they are consistent. This selection is based on the criteria that too small Watermark signal is vulnerable to attack and too large watermark signal takes large computer power.

Embedding watermark signal Xs into message M involves selecting a random block of m non-overlapping continuous rows and averaging these m rows to find average row vector R referred to as reference vector. Original watermark signal Xs is orthogonalized with respect to vector R to make inserted signal independent from the reference signal and eliminate cross talk [18]. Thus, the vector Ws' constructed out of W entries by modulating digital signature is [12, 19, 20]

$$Ws' = Xs - (Xs.\hat{R})\hat{R} \qquad (5)$$

A gain factor is calculated from Ws' across all m rows to ensure that strength of the watermark varies smoothly.

$$Ii = c\cos(2\pi i / m)\, Ws' \qquad (6)$$

Value of c is adjusted to maintain quality metric PSNR to minimum 30 DB, to avoid white visible marks on message signal. This small scaled version of the Ws' is added back to m rows of the original signal to generate watermarked signal M', where value of the bit function f' (x, y) is given as.

$$\bigcup_{r=i}^{i+m} f'(x_{r,} y) = \bigcup_{r=i}^{i+m} f(x_r, y) + I(x_{r-i}, y) \qquad 7(a)$$

$$\bigcup_{r=0}^{i-1} f'(x_{r,} y) = \bigcup_{r=0}^{i-1} f(x_r, y) \qquad 7(b)$$

$$\bigcup_{r=i+m+1}^{h-1} f'(x_{r,} y) = \bigcup_{r=i+m+1}^{h-1} f(x_r, y) \qquad 7(c)$$

where $0 \leq random(i) \leq w - m$

Other blocks of m rows can be selected pseudo randomly to embed additional watermarks using same Xs signal. All Xs and corresponding reference vectors are stored for detection purpose.

3.3 Encrypting watermark signal

RSA algorithm [5] is used to further encrypt watermarked signal M' using public key (d, n) of the receiver to achieve data integrity and confidentiality over network

$$M = \{f'(x, y) \mid x = 0 \text{ to width}, y = 0 \text{ to height}\}$$
$$C = M^d \bmod n \qquad (8)$$

4. Detection of Watermark to prove authenticity

The message received is decrypted using private key (e, n) of the receiver to assure for the sender that only authorized receiver can access message and data in the message has not been modified during transmission. To assure the receiver that message has come from the authentic sender. The watermark inserted in the message is detected.

$$M = C^e \bmod n \qquad (9)$$

A detection criterion is established using correlation analysis [19, 20]. Watermark is detected using the reference vector R and the watermark vector Xs sent with message itself. Xs is orthogonalized with respect to R to obtain Ws. Watermarked message is scanned from starting in blocks of m rows. An average vector is calculated from each block and orthogonalized with respect to reference vector R to find expected watermark vector EWs. EWs is correlated with the watermark vector Ws to test relative closeness.

$$\cos\theta = \frac{EWs.Ws}{|EWs||Ws|} \qquad (10)$$

If correlation coefficient is above a threshold value (between 0.5 & 1) then received document contains the watermark and assumed to have sent by an authentic sender.

Hundreds of random watermarks are synthesized with the same spectral properties as Xs. Correlation of each of these watermarks is computed with watermarked image. If later and former correlations are far apart it is likely that image contains watermark.

5 Verification to prove ownership

Figure 3 presents the procedure to protect rights of sender by deriving watermark from the watermarked image of the signal. Signature derivation will prove ownership of the sender if message is redistributed. At the same time it will restrict authorized receiver to illegally modify the message because in case of modification extracted signature will not match with the original signature of the sender.

Claimant can prove the ownership by presenting original image and the position where watermark was inserted. Gain factor is constructed by subtracting original image from watermarked image and orthogonal watermark Ws $^{/}$ is also constructed.

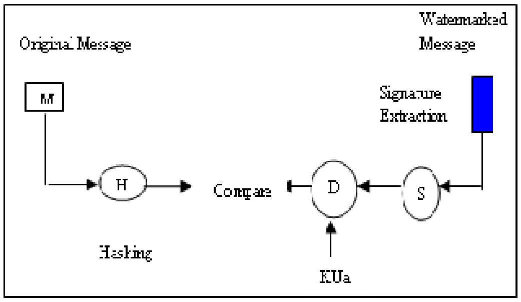


Figure 3: Detection & verification of signature

Vector triple product is applied to find value of Xs from equation (5).

$$(Xs \times \hat{R}) \times \hat{R} = (Xs \,.\, \hat{R})\,\hat{R} - (\hat{R}.\ \hat{R}\,)\,Xs \tag{11}$$

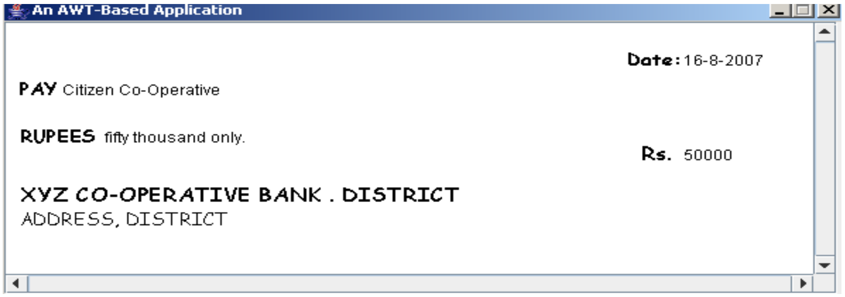
$$\begin{pmatrix} 1-\frac{a_1^2}{m_a^2} & \frac{a_1 a_2}{m_a} & \frac{a_1 a_3}{m_a} & \text{—} & \frac{a_1 a_n}{m_a} \\ \frac{a_2 a_1}{m_a} & 1-\frac{a_2^2}{m_a^2} & \frac{a_2 a_1}{m_a} & \text{—} & \frac{a_2 a_n}{m_a} \\ \frac{a_3 a_1}{m_a} & \frac{a_3 a_2}{m_a} & 1-\frac{a_3^2}{m_a^2} & \text{——} & \frac{a_3 a_n}{m_a} \\ \text{------} & \text{------} & \text{------} & & \\ \frac{a_n a_1}{m_a} & \frac{a_n a_2}{m_a} & \frac{a_n a_3}{m_a} & \text{—} & 1-\frac{a^2}{m_a^2} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \\ v_n \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ \\ w_n \end{pmatrix} \tag{12}$$

Gauss Jordan method is applied to equation (12) to find components of vector Xs., where m_r is length of vector R. Digital signature S of sender is constructed from Xs after removing all modulations and transformations. If, S and Xs are same, ownership of the sender is proved.

6 Implementation and Results

In this section we present the simulation results by implementing orthogonal signals based public-key watermarking algorithm.. We used a 32-bit RGB model to represent the cheque image using JAVA advanced imaging classes. We used SHA-1 algorithm to find message digest and RSA algorithm to encrypt message digest. We orthogonalized signature with respect to average vector found from selected block and embedded a scaled version of orthogonalized signature back to the selected block. PSNR was set to minimum 30 DB to avoid white noise. Overall image was encrypted with public key of the recipient to achieve confidentiality and integrity. Signature was detected using correlation analysis. Figure 4 shows 32-bit raster image of the document. Figure 5 shows watermarked image with PSNR 76DB and figure 6 shows the decrypted image. This image is used to detect the watermark using correlation.

The performance of the proposed algorithm is shown in figure 7. Correlation factor is found corresponding to the true signature derived from the original document and corresponding to the 100 randomly selected signatures. The correlation factor corresponding to true signature is between 0.9 and correlation factor corresponding to false signatures is negative or below 0.6.



Date:16-8-2007

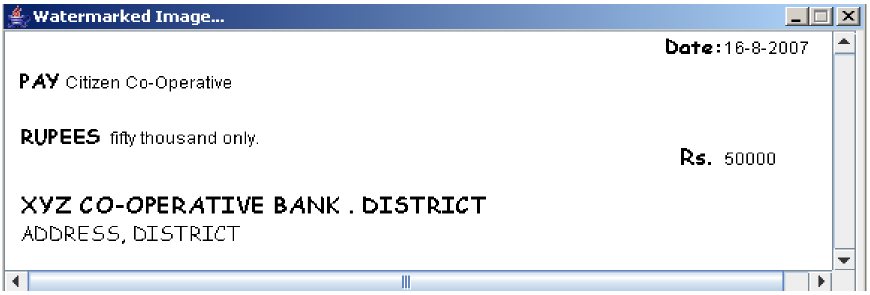
PAY Citizen Co-Operative

RUPEES fifty thousand only.

Rs. 50000

XYZ CO-OPERATIVE BANK . DISTRICT
ADDRESS, DISTRICT

Figure 4: Original Cheque Image



Date:16-8-2007

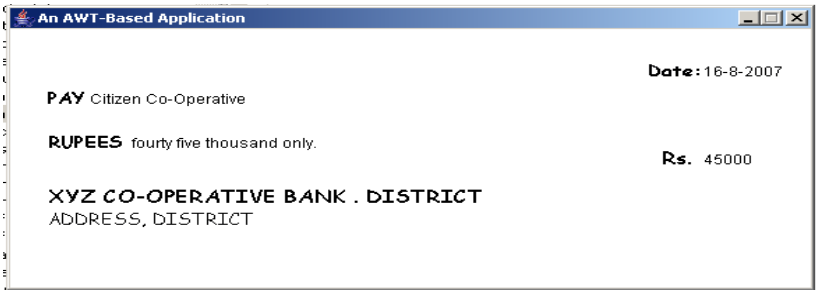
PAY Citizen Co-Operative

RUPEES fifty thousand only.

Rs. 50000

XYZ CO-OPERATIVE BANK . DISTRICT
ADDRESS, DISTRICT

Figure 5: Image of with embedded signature (PSNR -76.98141537143279)



Date:16-8-2007

PAY Citizen Co-Operative

RUPEES fourty five thousand only.

Rs. 45000

XYZ CO-OPERATIVE BANK . DISTRICT
ADDRESS, DISTRICT

Figure6 6: Received & Decrypted image

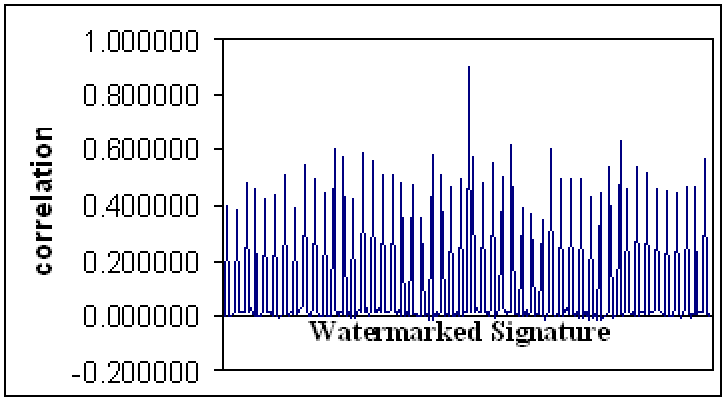


Figure 7: Correlation spread of watermarked image. Central spike corresponds to true signature and other points to randomly generated candidate signature

7 Conclusions

Most of the trading, banking and investment applications are based on exchanging structured documents over global network. For technical excellence and business values of these applications, security of information and sender's rights on information plays an essential role in overall transmission system. Cryptography alone can be an effective solution to all these problems but in most of instances in the form of costly and specialized hardware to create tamper proof devices. In this paper we have presented a software-based approach, which combines digital signature technology with robust watermarking technique to achieve authenticity, confidentiality, integrity and restricting alteration and forgery in information. The proposed technique is tested to prevent forgery of signature and alteration of information in cheques.

References

[1] Frank Hartung and Martin Kutter , " Multimedia Watermarking techniques", Proceeding of the Vol. 87, No. 7, July, 1999.

[2] Rivest. R , "The MD4 Message Digest Algorithm 1320" MIT and RSA Data Security Inc, April 1992.

[3] National Institute of Standards and Technology, Fips 180, Federal Information Processing Standards, Secure Hash Standard (SHS), April 1993.

[4] D.Eastlake .3rd, P.Jones.US , " Secure Hash Algorithm-1(SHA-1), September,2001.

[5] W. Stalling , " Cryptography and network Security Principles and Practice, 4th Edition", Prentice Hall.

[6] J.T. Brassil, S. Low and N.F. Maxemchak , " Electronic Marking and Identification Techniques to Discourage Document copying", IEEE journal on Selected Areas of Communication,,Vol.13, No. 8,October 1995.

[7] J.T. Brassil, S.Low and N.F.maxemchak , " Cpoyright Protection for the Electronic Distribution of text Documents", proceeding of the IEEE

[8] N.F. maxemchak and S.Low, " Marking Text Documents", Proceeding of the IEEE International Conference on Image Processing, Washington. DC, October 26-29, 1997, pp 13-16.

[9] Tao Chen, Jingchun Wang and Yonglei Zhou, " Combined Digital Signature and Digital Watermarking scheme for Image Authentication", in proc IEEE, international Conferences on Info-Tech& Info-Net (ICII2001), Vol 5, pp78-82, 2001.

[10] Ding Huang, " Inter word distance changes represented by sine waves for watermarking text images", IEEE transaction Circuits System Video tech (12), 1237-1245, 2001.

[11] Ji-Hong Chang and Long-Wen Chang, " A New Image copyright Protection Algorithm Using Digital Signature of Trading Message and Bar Code Watermark", Image and Vision Computing 03 New Zeeland Proceedings, 26-28, November, 2003.

[12] Con et al ,"Secure Spread Spectrum Watermarking for Multimedia", pp 1-33, Copyright, NEC Research Institute, Tech Report95-10.

[13] Balas Natrajan, " Robust Public-Key Watermarking of Digital Images", Computer Systems Laboratory, HPL, 97-118, October 1997.

[14] D.F.Rogers and J.A.Adams , " Mathematical Elements for Computer graphics", TATA-McGraw-Hill, Edition,2002.

[15] Daniel Sage & Michael Unser , " Teaching Image Processing programming in JAVA", IEEE Signal Processing Magazine, November 2003, pp 40-52.

[16] D. Sage, M User, " Easy JAVA Programming for Teaching Image Processing", Proc. Of the 2001 IEEE International Conference on Image Processing (ICIP01) , Thessalonica, Greece, 2001, Vol. 3, pp 298-301.

[17] D. Roman, M. Fischer and J. Cubillo , "Digital image Processing-An Object-Oriented approach," IEEE trans. Educ., Vol. 4, pp. 331-333,1998.

[18] William K. Pratt, "Digital Image Processing, (Fourth Edition), " pages 147 - 164. Copyright © 2007 John Wiley & Sons, Inc.

[19] B.P.Lathi, "Modern Digital and Analog communication system," Oxford University Press, third edition, 1998, pp 406-416.

[20] Rafael.C Gonzalez, Richard. E.Woods , " Digital image processing "Person education, seventh edition(2001), pp111.