Chapter XXI
Secure Image Archiving Using Novel Digital Watermarking Techniques

Ruo Ando
Keio University, Japan

Yoshiyasu Takefuji
Keio University, Japan

ABSTRACT

With the rapid advance in digital network, digital libraries, and particularly WWW (World Wide Web) services, we can retrieve many kinds of images on personal and mobile computer anytime and anywhere. At the same time, secure image archiving is becoming a major research area because the serious concern is raised about copyright protection and authority identification in digital media. A more sophisticated technique is required for future multimedia copyright protection. In this chapter we propose a secure image archiving using novel digital-watermarking techniques. Firstly, a nonlinear adaptive system (neural network) is applied for frequency-based digital watermarking. Secondly, we discuss application-oriented watermarking method for GIS image archiving. This chapter is divided into two parts. First section is about the way to apply nonlinear adaptive system for frequency-based image watermarking. We propose a new asymmetric technique employing nonlinear adaptive system trained on frequency domain. Our system uses two public keys to prevent removal attack and archive more fragile watermarking. In embedding, location information of frequency domain, where adaptive system is trained, is binalized, expressed in hexadecimal number, and encrypted in asymmetric cryptosystem. Encrypted location information is embedded in several parts of digital host contents. In generating key, supervised neural networks learn to assign the array of coefficients to teacher signal corresponding to the message to insert. This is one kind of transform-based method to generate public key from private key. In extracting, we use key matrix created by one-way signal processing of adaptive system. Proposal *method is tested in still image, and we have empirically obtained the results that the proposal model is functional in implementing more secure and fragile watermarking compared with previous techniques, such as correlation and transform-based asymmetric watermarking. Several experiments are reported to validate the effectiveness of our watermarking method. Second section is about the application of GIS image archiving using digital watermarking technique. Recently, the utilization of GIS (geographical information system) is becoming rapidly pervasive. Consequently, new methodology of archiving and managing images is a pressing problem for GIS users. It is also expected that as the utilization of GIS becomes widely spread, protecting copyright and confidential images will be more important. In this chapter, we propose a three-layer image data format that makes it possible to synthesize two kinds of related images and analysis information in one image data size. To achieve the confidentiality of one hidden image, we apply the private watermarking scheme, where the algorithm is closed to the public. In the proposal model, encoder netlist embedded in the third layer is generated by FOL prover to achieve more secure and less information to decode it, compared with one operation of another block cipher such as RSA. Proposal system users can process two images without the cost of maintaining key and decoding operation.*

INTRODUCTION

With the rapid advance in digital network, digital libraries, and particularly WWW (World Wide Web) services, digital watermarking is becoming a major research area because the serious concern is raised about copyright protection and authority identification in digital media. A more sophisticated technique is required for future multimedia copyright protection. Digital multimedia contents on the Internet are easily distributed, reproduced, and manipulated, compared with conventional analog data. In general, a digital watermark is a concealed code embedded into digital multimedia contents irremovably and imperceptibly in order to protect intellectual propriety rights. This chapter presents a new model of processing coefficients using supervised neural network. In our model, neural network is trained to assign coefficients to predefined secret code. Classification method of neural network can deal with predefined data, so it can detect weaker signal and figure out accurate recognition.

Geographical information systems (GIS) is a technological field under rapid progress that combines graphical features and tabular data according to the positions of the earth's surface. The prototype of GIS, which made it possible to program maps and store them on a computer for future modification if necessary, began around 1960. Currently, GIS are represented by several layers for manipulating, analyzing, and displaying for effective planning. The concept of overlaying different mapped features caused the situation that GIS is utilized for handling several maps. Consequently, in the process of GIS, overlaying and derivation are operated. As analysis of geographical images is becoming elaborate and complicated with the improvement of GIS, these bottlenecks are considered for further effective analysis and planning

Problem 1: Cost in managing image data. GIS image is analyzed and processed for a variety of purposes to generate the clipped or derived images. Also, the image is composed from many kinds of layer images for a particular valid analysis. Thumbnail images generated on the process of its use are rapidly increasing. As a result, the effective management of GIS image data is becoming apressing requirement. Usually header information and database are constructed separately, which costs to maintain and update these optional data.

Problem 2: Accessibility on the process of analysis. For GIS users, there are many situations that people have to discuss a particular area by considering several GIS images. In this case, maintaining the log of processing images and results of analysis is very important for effective research.

RELATED WORK

Digital watermarks can be divided into the following two points. At first, it could be categorized according to whether it uses an original image or not. Private (nonblind) watermarking needs the original data. This technique depends on the prewatermarked images to detect hidden code. Public (blind) watermarking requires performance without original image and watermark. Blind watermarking tends to be less robust and the most challenging method. Secondly, in embedding the hidden message, we should select the domain to process, that is, spatial domain and frequency domain. In spatial watermarking, the secret code is added to the spatial domain. Spatial watermark is easy to implement in the sense that it is embedded directly into an image's pixel data. On the other hand, frequency watermarking is based on some transform method such as FFT, DCT, and DWT (Craver & Katzenbeisser, 2001). Techniques in frequency domain are robust because they rely on the perceptual model of human vision. Recently, statistical models for coefficients in frequency domain have been proposed, such as Gaussian, Laplacian, and generalized Gaussian.

The research in GIS is classified into several fields, such as database modeling, simulation, image processing, and software engineering. GIS database is divided into modeling, which deals with effective data structure (Eggers, Su, & Girod, 2000), and recognition and retrieval system and analysis. The feature extraction from image is applying frequency transform such as DCT and DWT (Hachez & Quisquater, 2002). Recently, image processing of multispectrum sensing data is one of the major topics in GIS analysis (Cox, Kilian, Leighton, & Shamoon, 1997). Along with the popularization of Internet, recently, Web-based GIS management systems are expected to be more effective tools for data sharing and collection (Lin & Chang, 2000). As utilization of GIS is widely spread, some security problems such as protection of the copyright and confidential datas are more focused. Besides the security purpose, the digital watermarking is used in image classification (Kundur & Hatzinakos, 1997).

Asymmetric Watermarking

Digital watermarking is classified into two categories, according to the information disclosed for detectors: symmetric and asymmetric watermarking. In simple meaning, asymmetric watermarking is the technique using different types of keys. Traditional watermarking employs a symmetric scheme that requires the same key in embedding and detecting. The keys we need for message hiding and extraction are identical. So these conventional systems require the key for embedding watermark is disclosed completely in the verification process. This causes a security problem once attackers have signals similar to the embedding keys. They can easily remove the watermarks from the marked works by subtraction attack. In an asymmetric key cryptosystem, it must be almost impossible, even with current high performance computation, to deduce the private key from the public key. Therefore, an advantage of asymmetric watermarking is that the information about decoding key is not enough to remove watermark and that estimation of the secret message is not sufficient to eliminate watermark. As long as the some relation properties of embedded signal are satisfied, different watermarks can be used for many kinds of content. Consequently, the scheme is particularly secure to averaging attack.

Furthermore, asymmetric watermark is classified into two methods, watermark–characteristics-based method and transform-based method. Transform-based method is generating a detection key from previously defined key by some proper transform.Rrecently, many algorithms to render asymmetry were suggested; for example, eigenvector network, periodic watermark, neural network system, and so forth. Furon and Duhamel concluded from comparisons to public key cryptosystems that a one-way signal processing function is needed to build an asymmetric watermarking scheme. An asymmetric watermarking scheme has been defined as one for which the encryption key is different to the decoding key. Hence, the knowledge of the decoding key is not sufficient to remove the watermark. The security of the scheme presented here depends on the permutation, which is identical in both the embedder and detector. The scheme does not satisfy the requirements of a truly asymmetric scheme in that knowledge of the permutation key will allow attackers to destroy the watermark. Nevertheless, this scheme does not exhibit some of the important characteristics of asymmetric watermarking schemes. In particular, the detector is not dependent on any particular watermark signal, provided the correlation properties of the watermark are satisfied. In the current state of the art, a truly asymmetric public-key watermarking scheme remains to be found, and no scheme can afford to make all its detection parameters public. The extra security provided by our scheme therefore makes it an attractive option, provided that the private key can be kept secret. An advantage of this scheme is that estimation of the watermark by collusion attack is rendered impossible, so that the overall system is more secure. Knowledge of the public key does not enable an attacker to remove a watermark. More specifically, the public key must not reveal the location of the watermark in the cover. It must be computationally infeasible to deduce the private key from the public key.

Fragile Watermarking

Digital watermarking is classified into two categories according to the purpose: robust and fragile watermarking. In copyright protection, the robust watermark is applied to prove the origin even after some manipulation or alteration. Robust digital watermarks are used to provide a mechanism for copyright protection of digital contents by embedding authors and customer information. Robust watermark is also called copyright or fingerprint watermark. This watermark is for the contents that could be transferred, filtered, and compressed, owing to the user's purposes. Robust watermarks must be robust to many kinds of attacks, such as resizing, cropping, and filtering. To survive these attacks, current watermark schemes usually employ a spread spectrum approach.

In authentication applications of multimedia contents, the main purpose is to find the modification of data. The fragile watermark is designed for the objectives for authentication and integrity for host contents. This is an authentication technique to insert a signature designed to be undetectable after even slight manipulation of the content. So, fragile watermark is best used for protection and verification of original documents. As we discussed, in this chapter, the authentication of images is focused. Cryptography is probably the most common method used to authenticate the integrity of digital data. Cryptography is a traditional authentication method to conceal the message to an unauthorized person. In cryptography, digital signature preserves confidentiality and integrity. The signature is added to the encrypted message.

Fragile watermark is surely similar to cryptography, but can protect content by placing hidden information in the parts of content where it is not eliminated in normal usage. Fragile watermarking method takes advantages in inserting secret messages directly with no additional information to authenticate, while digital signature needs extra data transportation.

HVS Watermarking

A good watermark is supposed to be detectable by human sense, and can only be perceived by computing the correlation or periodicity. A recent watermarking method applies human visual system (HVS) features to insert signatures into host images. The actual human visual system is very complicated, and can process vast information. Roughly speaking, it is composed of a receiver with a preprocessing stage, the eye and the retina, a transmission channel, the optic nerve, and a processing engine, the visual cortex. But in frequency domain, HVS are less sensitive in textured, edge, and rapid-changing regions. This characteristic makes these zones appropriate for embedding watermark. Psychophysical experiments have shown that the response of visual cortex is turned to the band-limited portion of the frequency domain. It gives evidence that the brain decomposes the spectra into perceptual channels that are bands in spatial frequency. Now HVS is a reasonable standard in measuring whether the media contents are tampered with or not, since our eyes are sensitive to modifications beyond perception.

As we discussed before, a good watermark is supposed to be invisible for human eyes and undetectable without information to detect. Also, it should remain in spite of spatial/temporal modification. To satisfy these requirements, a watermark using human visual system (HVS) has been proposed (Podilchuk & Zeng, 1998). According to HVS, human eyes are less accurate in the regions where the change is rapid, which make preferable zones to watermark. On the other hand, human visual system is sensitive in the regions where the value is changed smoothly, which in turn is not proper to embed the secret message.

Compared with previous watermarking techniques using global information, the adaptive watermarking based on HVS selects the appropriate parts of frequency domain, where the message will be imperceptible and robust for some changes (Kwon, Kwon, Nam, & Tewfik, 2002).

This content-adaptive watermarking has been researched mainly using a stochastic model based on frequency transform. They utilize the local properties of contents to select the optimal embedding blocks with following subband quantization and perceptual model. (Kundur & Hatzinakos, 1997).

Proposal Watermarking Scheme

In proposal method, we embed and detect location value. Location value is processed as input signal with nonlinear adaptive system, such as back propagation network. In inserting watermark, a key is generated. Compared with conventional model where signature is equivalent to the message to hide, we embed location code and train nonlinear adaptive system, such as neural networks, with teacher signal corresponding to secret message. In detecting secret message, output signal is converted to bit code, according to threshold (about more than 0.95). We can extract the secret message by processing input signal of the blocks where location value is indicating.

Our model is asymmetric in two meanings. First, location code is encrypted with private key and decrypted with public key. Second, the key to extract hidden bit code is transformed by one-way signal processing of neural network. To achieve more secure watermarking, location value is encrypted. In symmetric watermarks, attackers can remove watermarking. We apply asymmetric watermarking and encrypt location code with private key. In detection, we can decrypt location code with public key. Consequently, we have two keys to extract watermarks.

Compared with using ASCII code, location value embedding renders shorter code to insert. And all characters are assigned to 3 bit constantly. The code to insert is encrypted with private key, and we obtain more secure processing of asymmetric watermarking. In proposal method, the range of location value is from 0 to 7, because we use discrete cosign transform with blocks 8*8. Location value is expressed in hexadecimal number. In hexadecimal number, one bit change may cause bigger changes in decimal number.

The schematic diagram of embedding process is depicted in figure.

Watermark embedding process is divided into two steps: (1) embedding and (2) key generation. As we mentioned before, transform-based method to make a detection key from a given embedding key by proper transform is applied. In encryption

Figure 1. Embedding watermark

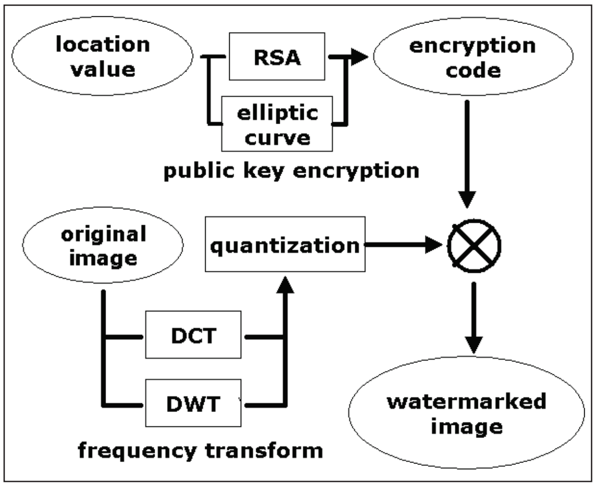
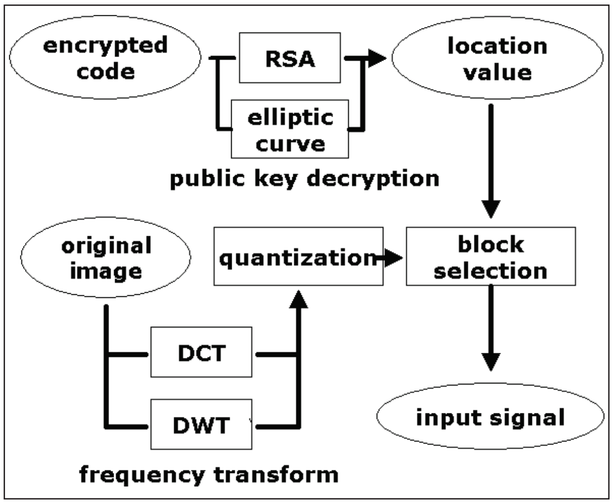


Figure 2 Detecting watermark



of location value, we use private key of RSA. But in generating key, we generate the key from location value by training nonlinear adaptive system. Consequently, we use two keys to extract hidden information. The schematic diagram of extraction process is illustrated in Figure 2.

In proposal model, extraction process is feed-forward, computing with input signal of the coefficients of the DCT/DWT blocks. We applied recognition process on frequency domain, and convert analog output signal to bit code. Extraction process is divided into two processes. First, we decrypt the location value with public key. Second, we set the input signal as the coefficients of the DCT block the decrypted value indicated. We use asymmetric cryptosystem because complete information disclosure of location value causes the possibility of removal attacks such as averaging attack. The details of each step are described in the following section.

Location Code Encryption

The proposal model aims for asymmetric and fragile watermarking. This step is concerned with asymmetric watermarking. To avoid removal attack, we use asymmetric cryptography for location value. In this chapter we applied RSA algorithms discussed in section 3.1 to encrypt location value.

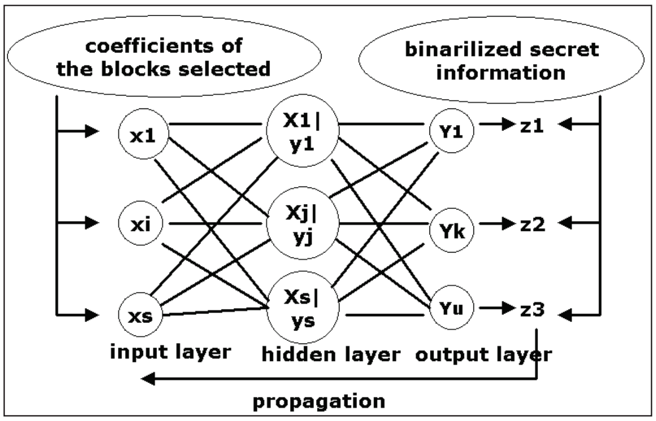
ADAPTIVE WATERMARKING AND KEY GENERATION USING NEURAL NETWORK

The adaptive watermarking based on HVS select the appropriate parts of frequency domain, where the message will be imperceptible and robust for some changes.

Watermark should be undetectable without key. In this case, the key is equivalent to connection weight matrix of back propagation. As shown in the figure, the supervised learning system process DCT coefficient as input signal. And in training, the hidden inserted is binalized as fixed output to neural net. Once the location value is embedded, the connection weight matrix is utilized as key to extract hidden code. In other words, learning process of neural network is transform process to generate key; connection weight matrix should be saved as key.

- **Step 1:** Calculate the DCT coefficients for each 8*8 block.
- **Step 2:** Quantize the DCT coefficients by standard JPEG quantization table.

Figure 3. Key generation. Asymmetric rendering



- **Step 3:** Select the DCT block.
- **Step 4:** Embed the encrypted value in selected block.
- **Step 5:** Train the supervised neural network with the teacher signal corresponding to secret bit code. Input signals are the coefficients of DCT block.

In processing on frequency domain, neural network takes advantages in calculating mainly in two aspects. (1) Neural network is a nonlinear system that is able to process the nonlinear behavior well. (2) Neural network has fault tolerance, that is, the network can continue to perform acceptably in spite of the failure of some elements in the network.

Location Code Decryption

Extraction step is divided into two steps: location code decryption and nonlinear signal processing. In this step, location value is decrypted with public key. In embedding, location value is expressed in hexadecimal code. So, if some manipulation is operated on host images, decrypted location value is changed.

Watermark Extraction

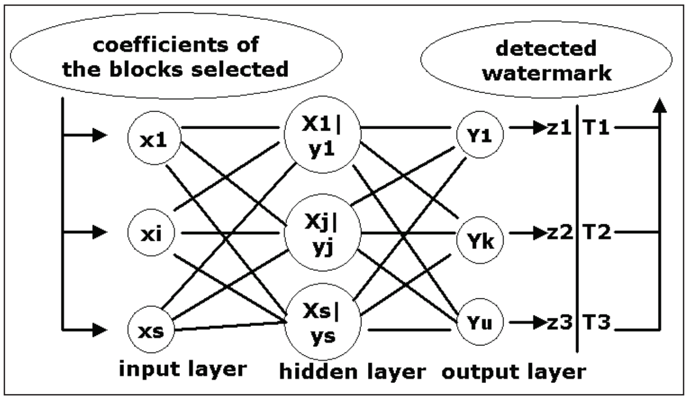
In extraction of watermarks, we need:

1. Information about the location of blocks where the neural network was trained.
2. Public key.
3. Connection weight matrix as key. Steps to detect watermark is as follows:
   - **Step 1:** Calculate the DCT coefficients for each 8*8 block.
   - **Step 2:** Quantize the DCT coefficients by standard JPEG qauntization table.
   - **Step 3:** Process input signal. Input signals are the coefficients of the block selected.

In this phase, recognition is processed by forward phase in backpropagation computing. In forwarding computation, the input signal is propagated from layer to layer in network, with the parameters fixed. This recognition phase is finished when each signal of the output layer is figured out.

1. Compared with using ASCII code, location value embedding renders shorter code to insert.

Figure 4. Watermark extraction



2. The code to insert is encrypted with private key, and we obtain security of asymmetric watermarking.
3. In proposal method, the range of location value is from 0 to 7 because we use DCT. Location value is expressed in hexadecimal number. In hexadecimal number, one-bit changes may be big changes compared with decimal number.
4. In proposal method, the range of location value is from 0 to 7 because we use DCT. Location value is expressed in hexadecimal number. In hexadecimal number, one-bit changes may be big changes compared with decimal number. 3.1 RSA

RSA is a public-key cryptosystem implemented for both encryption and authentication on Internet. It was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

The steps of RSA are as follows:

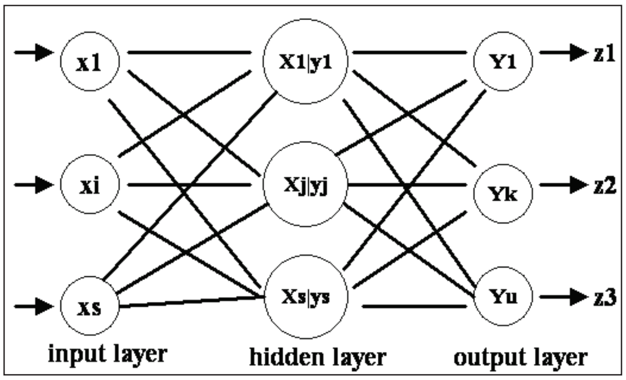
1. The process begins to select P and Q, two large prime numbers (hundreds of digits).
2. Choose E such that E and $(P - 1)(Q - 1)$ are relatively prime, which means they have no prime factors in common. E does not have to be prime, but it must be odd. $(P - 1)(Q - 1)$ cannot be prime because it is an even number.
3. Find out D, its inverse, and mod $(P - 1)(Q - 1)$ so that $(DE - 1)$ is divisible by $(P - 1)(Q - 1)$.
   This could be written as:
   $DE = 1 \bmod (P - 1)(Q - 1)$, and D is called as the multiplicative inverse of E.
4. Once these steps are done, message can be encrypted in blocks, and manipulated on the following:
   where T is the plaintext (a positive number)
5. Similarly, C is decrypted through the following equation.
   where C is the cipher text (a positive number)

It is impossible to deduce the private key from the public key. The cipher text can be decrypted only by corresponding private key. The public key is the pair (PQ, E). The primitive number D computed in Step 3 must not be revealed to anyone. The product PQ is called the modulus. E selected in Step 2 is the public exponent. We also call D as the decryption or secret exponent.

BACK PROPAGATION NETWORK

Backpropagation is the supervised learning algorithm of feed-forward neural network. This algorithm is processed in four steps: initialization, presentations of training examples, forward

Figure 5. Backpropagation network



computation, and backward computation. In backward computation, we use the delta rule to modify connection weight of each neuron.

THREE LAYER IMAGE DATA STRUCTURE

Three layer image data structure is watermark-based technology that embeds two images and one archiving information header into a single image. In the figure, biotope map and header information is watermarked into the aerial image. This method relies on human visual system (HVS) watermarking, which is supposed to be invisible for human eyes and undetectable without information to detect. Aerial image and biotope map are usually analyzed by human experts. Consequently, it is possible to synthesize two images and its archiving header into one image without loss of effectiveness of analysis. As shown in the figure, three layer images are decomposed into eight layer as follows:

- **Layer [0]-[3]:** Assigned for aerial image data.
- **Layer [4]:** Header (archiving information and processing log).
- **Layer [5]-[7]:** Assigned for biotope map data.

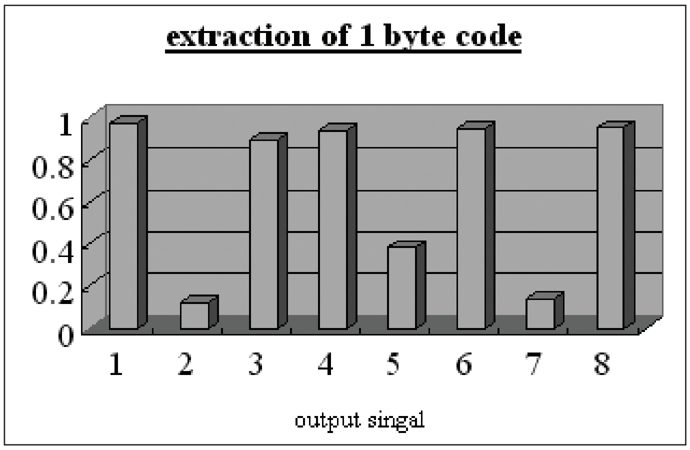
Based on HVS watermarking techniques, users can analyze these two images while maintaining reasonable quality for analysis. Besides, it is possible to retrieve logs to process and archive without database and searching.

Experimental Results

To test this algorithm, we implemented a system for embedding and restoring 8 bits in images of size 256*256. We computed the DCT coefficients for each 8*8 block, and quantized those values by standard JPEG quantization table. In embedding the location value and training network, we set 8 perceptrons of input and output layer. In training network, we set the teacher signal (1,0,1,1,0,1,0,1).

Figure 4 shows the result of processing coefficients of the block selected correctly. The output of processing coefficients in irrelevant block is shown in Figure 5. Extraction failed when we selected the arrays of coefficients that were not processed as input signal in supervised learning.

Figure 6. Output signal by processing in the selected block



In learning process, we prepare several insignificant patterns that all coefficients are extremely high or low, and train the network in order to assign these patterns to teacher signal such as (0,0,0,0,0,0,0,0) or (1,1,1,1,1,1,1,1). Experimental results show that our method is functional in recognizing the block that is not selected as a meaningless array, and in avoiding unexpected extraction from the incorrect blocks.

As we know, in proposal model, the location value is encrypted and embedded. Figure 8. shows the bit loss rate. The coefficients of high-frequency domain are modified to binary number 0/1. After filters listed in Figure 8, almost

Figure 7. Output signal by processing in the block where the network was not trained

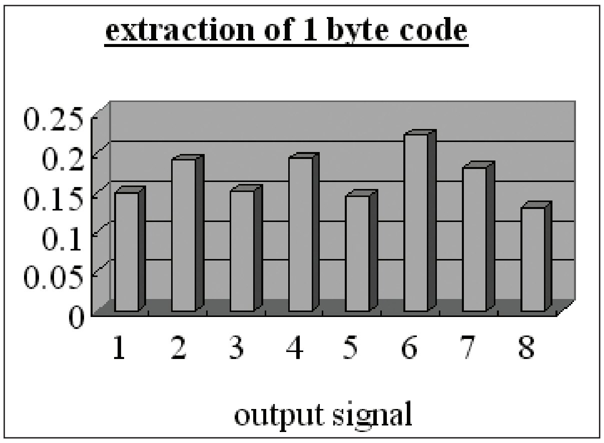
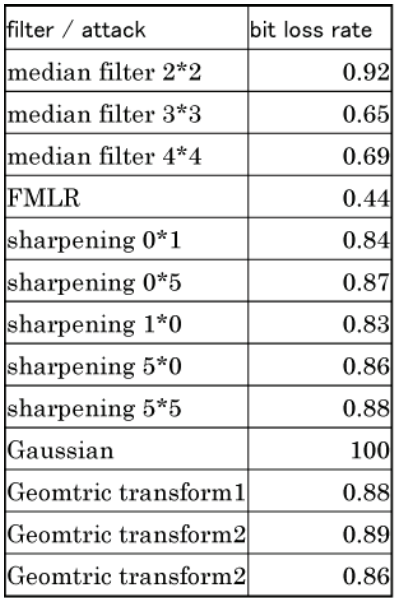


Figure 8. Bit loss rate after filters/attacks. Location value cannot be restored



filter / attack	bit loss rate
median filter 2*2	0.92
median filter 3*3	0.65
median filter 4*4	0.69
FMLR	0.44
sharpening 0*1	0.84
sharpening 0*5	0.87
sharpening 1*0	0.83
sharpening 5*0	0.86
sharpening 5*5	0.88
Gaussian	100
Geomtric transform1	0.88
Geomtric transform2	0.89
Geomtric transform2	0.86

all location information expressed by binarized and hexadecimal number has become unable to be restored. We have obtained the results that compared with correlation-based extraction, our method is more fragile in the sense that location information breaks down, for nonlinear adaptive systems output, the signals near (0,0,0,0,0,0,0,0), as shown in Figure 7.

To eliminate the watermark, filtering images may be attempted. For filtering attacks, our watermarking is robust because one location value is concealed in several pixels, as we discussed in section 3. In the proposal method, even when an attacker still intends to eliminate watermarks without the key, he must filter the images to the extent that the many features of image are lost or broken. This means that the image is not valuable for attackers also. Figure 6. shows experimental evaluation of robustness after the high-pass filter. In our experiment, less than 30% of location value is changed after this filter.

CONCLUSION

Based on HVS watermarking techniques, users can analyze these two images while maintaining reasonable quality for analysis. Besides, it is possible to retrieve logs to process and archive without database and searching. With the rapid advance in digital network, digital libraries, and particularly WWW (World Wide Web) services, we can retrieve many kinds of images on personal and mobile computer anytime and anywhere. At the same time, secure image archiving is becoming a major research area because the serious concern is raised about copyright protection and authority identification in digital media. In this chapter, we propose a secure image archiving using novel digital watermarking techniques. Firstly, nonlinear adaptive system (neural network) is applied for frequency-based digital watermarking. Secondly, we discuss application-oriented watermarking method for GIS image archiving. This chapter is divided into two parts. First section is about the way to apply nonlinear adaptive system for frequency-based image watermarking. We propose a new asymmetric technique employing nonlinear adaptive system trained on frequency domain. Our system uses two public keys to prevent removal attack and archive more fragile watermarking. In embedding, location information of frequency domain, where adaptive system is trained, is binarized, expressed in hexadecimal number, and encrypted in asymmetric cryptosystem. And encrypted location information is embedded in

Figure 9. Host images of experiment

several parts of digital host contents. In generating key, supervised neural networks learn to assign the array of coefficients to teacher signal corresponding to the message to insert. This is one kind of transform-based method to generate public key from private key. In extracting, we use key matrix created by one-way signal processing of adaptive system. Proposal method is tested in still image. And we have empirically obtained the results that the proposal model is functional in implementing more secure and fragile watermarking compared with previous techniques, such as correlation and transform-based asymmetric watermarking. Several experiments are reported to validate the effectiveness of our watermarking method. Second section is about the application of GIS image archiving using digital watermarking technique. Recently, the utilization of GIS (geographical information gystem) is becoming rapidly pervasive. Consequently, new methodology of archiving and managing images is a pressing problem for GIS users. It is also expected that as the utilization of GIS becomes wide spread, protecting copyright and confidential images will be more important. In this chapter, we propose a three-layer image data format that makes it possible to synthesize two kinds of related images and analysis information in one image data size. To achieve the confidentiality of one hidden image, we apply the private watermarking scheme, where algorithm is closed to the public. In the proposal model, encoder netlist embedded in the third layer is generated by FOL prover to achieve more secure and less information to decode it, compared with one operation of another block cipher such as RSA. Proposal system users can process two images without the cost of maintaining key and decoding operation.

REFERENCES

Abdi, H., Valentin, D., & Edelman, B. (1999). *Neural networks*. Thousand Oaks, CA: Sage.

Anderson, J. A. (1995). *An introduction to neural networks*.

Bertsekas, D.P. (1999). *Nonlinear programming*. Athena Scientific.

Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Trans. on Image Processing*, 1673-1687.

Craver, S., & Katzenbeisser, S. (2001). Copyright protection protocols based on asymmetric watermarking: The ticket concept. *Communications and Multimedia Security Issues of the New Century.* Kluwer Academic Publishers.

Eggers, J. J., Su, J. K. & Girod, B. (2000). Asymmetric watermarking schemes. *Tagungsband des GI Workshops Sicherheit in Mediendaten, Berlin, Germany.*

Fausett L. (1994). *Fundamentals of neural networks*. Arichtectures, algorithms, and applications. Englewood Cliffs, NJ: Prentice-Hall.

Fukushima, K. (1975). “Cognitron: A self-organizing multilayered neural network. *Biological Cybernetics, 20,* 121–136.

Hachez, G. ,& Quisquater, J. J. (2002). Which directions for asymmetric watermarking? In *Proceedings of the XI European Signal Processing Conference, EUSIPCO 2002.*

Hu, J., Huang, J., Huang, D., & Shi, Y. Q. (2002). A DWT-based fragile watermarking tolerant of JPEG compression. *IWDW 2002* (pp.179-188).

Hurley, N. J., & Silvestre, G.. C. M. (2002). Nth order audio watermarking. In E. J. Delp III, P. W. Wong (Eds.), *Security and Watermarking of Multimedia Contents IV Proceedings of SPIE, 4675*, 102-110.

Kim, T. Y., Kim, T., & Choi, H. (2003). Correlation-based asymmetric watermark detector.

International Conference on Information Technology: Coding and Computing (ITCC 2003. (pp.564-568).

Kundur, D., & Hatzinakos, D. (1997). A robust digital image watermarking method using wavelet-based fusion. In *Proceedings of the ICIP-97, 1,* 544-547.

Kwon, K. R., Kwon, S. G., Nam, J. H, & Tewfik, A. H. (2002). Content adaptive watermark embedding in the multiwavelet transform using as tochastic image model. *IWDW200,* (pp.249-263).

Lewis-Beck, M. S., Bryman, A. E., & Liao, F. (2003). *The SAGE encyclopedia of social science research methods*. Sage Publications.

Lin, C. Y., & Chang, S. F. (2000). Semi-fragile watermarking for authenticating JPEG visual content. *SPIE Security and Watermarking of Multimedia Content II, EI'00* (pp.140-151).

Marvel, L. M., Hartwig, G. W. Jr., & Boncelet, C. B. Jr. (2000). Compression-compatible fragile and semi-fragile tamper detection. *Proceedings of SPIE 3971,* (pp.131-139).

Podilchuk, C. J., & Zeng, W. (1998). Image-adaptive watermarking using visual models. *IEEE Journal on Selected Areas in Communications, 16*(4), 525-539.