Authentication Technologies of X-ray Inspection Image for Container Terminal Automation

Jong-Nam Kim, Jin-Ho Hwang, Tae-Kyung Ryu, Kwang-Seok Moon, Gwang S. Jung*

Div. of Electronic, Computer and Telecommunication Engineering, Pukyong National University, Busan, Korea
(jongnam@pknu.ac.kr, moonks@pknu.ac.kr)

* Dept. of Mathematics and Computer Science, Lehman College/CUNY, USA
(gwang.jung@lehman.cuny.edu)

Abstract: In this paper, authentication technologies for X-ray inspection images in container merchandises are introduced and a method of authentication for X-ray inspection images is proposed. Until now, X-ray images of container merchandises have been managed without any authentication of inspection results and environments, it means that there was no any action for protection of illegal copy and counterfeiting of X-ray images from inspection results. Here, authentication identifies that who did inspect container X-ray images and, whether the container X-ray images were counterfeited or not. Our proposed algorithm indicates to put important information about X-ray inspection results on an X-ray image without affecting quality of the original image. Therefore, this paper will be useful in determining an appropriate technology and system specification for authentication of X-ray inspection images. As a result of experiment, we find that the information can be embedded to X-ray image without large degradation of image quality. Our proposed algorithm has high detection ratio by Quality 20 of JPEG attack.

Keywords: image authentication, x-ray inspection, container terminal, data hiding, watermarking.

1. INTRODUCTION

With the development of modern economy of the whole world, containers are widely used to transport all kinds of goods. There are some researches about automation of container code identity, but there are hardly researches about X-ray inspection automation of container merchandise. In order to manage the containers efficiently, it should have more development in X-ray inspection automation of container merchandise. When the inspector finally confirms the passed image through the X-ray inspection, it should be authenticated by reliable technologies.

It is necessary to ensure the transparency for document preservation after processing, but it has been investigated that there was no such processing of container merchandises in home and abroad. If there is no final confirmation and authentication for the passed image through the X-ray inspection, we do not ensure the transparency of processed document preservation. And it can be processed unsuitably in X-ray inspection degree or can be hindrance in automation of X-ray inspection.

So, it has to preserve the information which is consisted of the image of X-ray inspection and the results of inspection. After authentication, it needs technologies which prevents from forgery and alteration.

The watermarking is prospective technology which combines original image as well as additional information of the user. This makes it hard to eliminate or forge the additional information of the user from others. The derivation of the watermark is a mark which is embedded transparently to discriminate paper manufacturer's own paper for 700 years ago, in the Italy.

The digital watermarking is to apply this to digital image and it conceals the information that cannot be recognized at digital image data. It is possible to use this unrecognizable information at copyright, ownership, limitation of usage. Furthermore it can be applied to monitoring, identification of ownership, property rights authentication, distribution tracking, copy protection and access control [1]-[4].

In this paper, authentication technologies for X-ray inspection images in container merchandises are introduced and a method of authentication for X-ray inspection images is proposed. Until now, X-ray images of container merchandises have been managed without any authentication of inspection results and environments, it means that there was no any action for protection of illegal copy and counterfeiting of X-ray images as inspection results. Here, authentication identifies who did inspect container X-ray images and, whether the container X-ray images were counterfeited or not. Our proposed algorithm indicates to put important information about X-ray inspection results on an X-ray image without affecting on original image. Therefore, this paper will be useful in determining an appropriate technology and system specification for authentication of X-ray inspection images.

2. IMAGE AUTHENTICATION TECHNOLOGIES USING WATERMARKING

In the early 1990, digital watermarking technology was introduced at first. Since the middle of 1990, a number of methods have been developed. Watermarking technology melts additional information of the user into original media. This makes the sense of human sight invisible and makes additional information of the user always existent in the media. At first it was developed for protection of the digital media copyright, but its application arranges are being extended.

Authentication watermarking is inserted a hidden data into an image in order to detect any alterations. A watermark is a signal added to digital data (audio, video and still images) that can be detected or extracted later to make an assertion about the data. Embedding a watermark in an image means inserting information in the image, such that the image quality does not deteriorate significantly. A watermark can be visible or invisible. A visible watermark typically contains a visual message or a company logo that indicates the ownership of the image. An invisible watermarked image is visually very similar to the original image. The existence of such a watermark can be determined only through a watermark extraction or detection algorithm. Invisible watermarking techniques can be classified as robust and fragile.

Robust watermarks are designed to be hard to remove and to resist common image-manipulation procedures. They are useful for copyright and ownership assertion purposes.

Fragile watermarks (or authentication watermarks) are easily corrupted by any image-processing. Watermarks for checking image integrity can be fragile because if the watermark is removed, the watermark detection algorithm will report the corruption of the image.

Halftoning is a process to convert a grayscale image *G* into corresponding binary image *B*, such that *B* looks like *G* when viewed from a distance. Classic halftone methods include ordered dithering, error diffusion and dot diffusion. Halftone images appear routinely in books, magazines, newspapers, printer outputs and fax documents. Halftone images can be dispersed-dot or clustered-dot. Usually, dispersed-dot has a better visual quality, but some devices cannot reproduce too-finely-dispersed dots (like laser printer) and they must use clustered-dot halftoning [5].

From these points of view, we can use variable watermarking as image authentication technology. With this, we can insert the information about inspection result to inspection image and do not make the information modified. Finally, we can make it to extract the inspection information and the system through these processes can preserve/manage the information about inspection securely.

Fig. 1 shows watermark procedure of embedding and extracting.

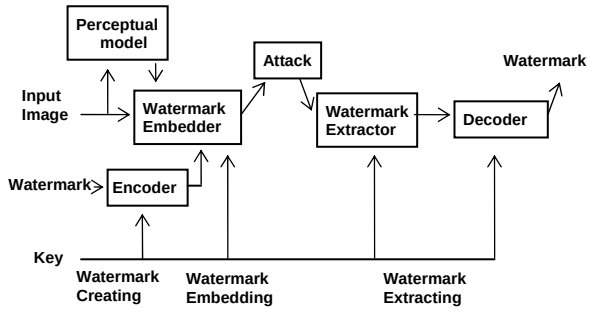

Fig.1 Procedure of image watermarking

Watermark embedding process is inserting created watermark to original image. Usually it uses a form to add for determining insertion strength in spatial domain or transform domain. Here, transform domain means DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and FMT (Fourier-Mellin Transform). According to usage purpose, variant domains are used [3]-[4].

Watermark extracting method has two forms, non-blind and blind. Non-blind method is regarded as to extract with original image and blind method is regarded as to do without it. Non-blind method process that use difference between original image and watermarked image. Blind methods are that use the autocorrelation of watermark signal, matched filter and MAP (Maximum A-Posteriori) of probable application.

From this point of view, watermarking technologies can be classified into two groups: estimation-based method and quantization-based method. Estimation-based method is to add or product the watermark to original data. This is not to extract directly but to extract after estimation of watermark signals or removal of original signals. This has robustness for attacks of variable kinds and high damage but it has a shortcoming in a little channel capacity. On the other hand, quantization-based method previously is designed to minimize effects of original data. It is robust for White-Gaussian-noise attack but it has no robustness for filtering attacks. In comparison with these methods, estimation-based method is often used for insertion of copyright information; the other is primarily used to hide data [3]-[4].

Based on these accessible methods, many watermarking technologies are being investigated and published till now. Starting from the scheme of watermark signal, technology researches are being investigated in many area that are modulation for more watermarking information, adjustment for insertion strength, consideration for watermark insertion area, correcting error for error information and extracting for mixed watermark image. Technologies that where watermark is embedded and what degree of watermark strength is embedded, are the most attractive to make it important issue. According to prior two conditions, it is determined whether human visual system feels the changes for watermarked image or not [6]-[7].

3. EMBEDDING AND DETECTION ALGORITHM

3.1 Embedding Algorithm

Our proposed algorithm can be implemented by blind watermarking and watermark takes anti-podal form for stability of extraction. Namely, in order to insert digital signal 0 and 1 it maps each values to -1 and 1. Detection ratio is improved rapidly because distance of signals is twice longer than prior method.

For this reason, we can use Hadamard matrix for watermark signal. Hadamard matrices may be defined as binary orthogonal matrices in which all parallel rows or columns are uncorrelated; i.e., the m^2 matrix $[h_{ij}]$ is a Hadamard matrix if all $h_{ij} = \pm 1$ and

$$\sum_i h_{ia} h_{ib} = \sum_j h_{aj} h_{bj} = m\delta_{ab} \tag{1}$$

Aside from the trivial cases of $m = 1$ and $m = 2$, these conditions can be satisfied only if m is a multiple of four [8].
Our proposed algorithm can use these characteristics for watermark. We regard each column (or row) as one symbol, it is used for watermark.

We use the watermark embedding model in additive form as follows:

$$\hat{I}_{n,m} = I_{n,m} + \alpha_{n,m} \cdot W_{n,m}, \tag{2}$$

$I_{n,m}$: original contents $\hat{I}_{n,m}$: watermarked contents
$\alpha_{n,m}$: watermark strength $W_{n,m}$: watermark

where $\alpha_{n,m}$ determines strength of watermark, this is important factor to adjust the trade-off between invisibility and robustness. If $\alpha_{n,m}$ has small value then it has no effect with image quality but the robustness of watermark is down. And if $\alpha_{n,m}$ has large value then it has a problem with degradation of image quality in flat region. Therefore $\alpha_{n,m}$ must have the adaptive value for consideration of local characteristic of

image. Using such image characteristic is the same as using HVS (Human Visual System).

Adaptively in order to embed watermark, prior to the embedding process, proposed algorithm uses pre-processing filter. After filtering, it can extract probable regions for strength of watermark. At this time, the filter coefficients use fixed coefficient values and it is working about power-spectrum of signal. Here, power-spectrum means power-spectrum of the signal which removed the local mean from original signal. Hence, estimation of watermark can be considered by Wiener filter [9]. For more details, it will be introduced in the next paragraph.

For invisible characteristic of HVS, $\alpha_{n,m}$ of flat area is sensitive to change, $\alpha_{n,m}$ of complex area is insensitive to change. Adjusting $\alpha_{n,m}$ by using thresholds about characteristic of local area, that is additive noises have each different values according to original signal even though they are same values.

Steps of embedding are performed as following;

1) Select embedding areas and make a watermark after determining Hadamard matrix size and random 8 symbols of it. Watermark is repeated as embedding area size and create hidden information $W_{n,m}$.
2) For determining α value, calculate the power spectrum of original image and according to 6 thresholds of the results watermark strength $\alpha_{n,m}$ is determined.

$$\alpha_{n,m} = \begin{cases} 1 \Rightarrow T_1 \le P_i(n,m) < T_2 \\ 2 \Rightarrow T_2 \le P_i(n,m) < T_3 \\ 3 \Rightarrow T_3 \le P_i(n,m) < T_4 \\ 4 \Rightarrow T_4 \le P_i(n,m) < T_5 \\ 5 \Rightarrow T_5 \le P_i(n,m) < T_6 \\ 6 \Rightarrow T_6 \le P_i(n,m) \end{cases} \quad (3)$$

where T_n is each threshold for determining $\alpha_{n,m}$, $P_i(n,m)$ is power-spectrum value about original image. Thus the value of $\alpha_{n,m}$ has between -6 and 6.

3) Make noise information, N which is the product of $\alpha_{n,m}$ by $W_{n,m}$. And add N to original image, $I_{n,m}$ as Eq. (2).

3.2 Detection Algorithm

Watermark of our detection method is estimated by using wiener filter which restores original signal from degraded signal. Fig. 2 shows the concept of Wiener filter.

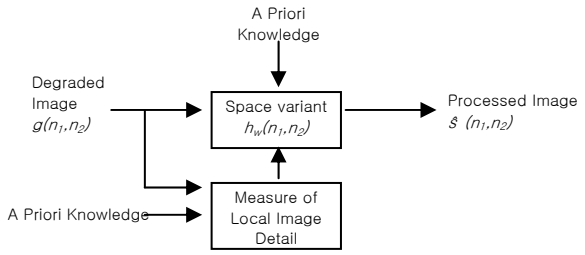

Fig.2 Concept of Wiener filter

Let us suppose that an image $s(n_1, n_2)$ is corrupted by additive zero-mean white noise $n(n_1,n_2)$ producing an observed image $g(n_1, n_2)$:

$$g(n_1, n_2) = s(n_1, n_2) + n(n_1, n_2) \quad (4)$$

$s(n_1, n_2)$ is assumed to be a two-dimensional zero-mean stationary random signal. We want to estimate image $\hat{s}(n_1, n_2)$ from the noisy observed image $g(n_1, n_2)$, by using a linear filter having impulse response $h_w(n_1, n_2)$:

$$\hat{s}(n_1, n_2) = g(n_1, n_2) * h_w(n_1, n_2) \quad (5)$$

It assumes that we know characteristic of statistic model about $s(n_1, n_2)$ and $n(n_1, n_2)$. If $g(n_1, n_2)$ pass the filter $h_w(n_1, n_2)$ which applied it, we can get $\hat{s}(n_1, n_2)$ which is estimation of $s(n_1, n_2)$. Wiener filter is composed the form which minimize the difference between $s(n_1, n_2)$ and $\hat{s}(n_1, n_2)$. The filter impulse response is chosen in such a way that the mean square error

$$E=E[|e(n_1, n_2)|^2]=E[|s(n_1, n_2) - \hat{s}(n_1, n_2)|^2] \quad (6)$$

is minimized. $E[\bullet]$ denotes the expectation operator. It is assumed that the noise and the image are uncorrelated. Based on this condition, it can be easily proven that the filter, which minimizes Eq. (6), we can get the filtered data, $\hat{s}(n_1, n_2)$, as follows:

m_f: mean of the signal in local area
m_v: mean of the noise in local area
$P_f(w_1, w_2)$: power spectrum of the signal in local area
$P_v(w_1, w_2)$: power spectrum of the noise in local area
$v(n_1, n_2)$: additive white Gaussian noise,
mean = 0 and dispersion = δ_v^2.

$$\hat{s}(n_1,n_2) = m_f + (g(n_1,n_2) - m_f) * \frac{\sigma_f^2}{\sigma_f^2 + \sigma_v^2} \quad (7)$$

Fig.3 shows the composition of the Wiener filter. At Eq.7 m_f equals to m_g as m_v is zero. i.e., it can solve $m_f(n_1,n_2)$ from $g(n_1,n_2)$.

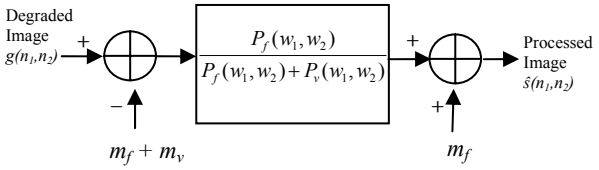

Fig.3 Composition of the Wiener filter

$$\hat{m}_f(n_1,n_2) = \frac{1}{(2M+1)^2} \sum_{k_1=n_1-M}^{n_1+M} \sum_{k_2=n_2-M}^{n_2+M} g(k_1,k_2) \quad (8)$$

Hence, the Wiener filter $h_w(n_1, n_2)$ can be found as following:

$$h(n_1,n_2)=\begin{cases}\dfrac{\sigma_f^2+\dfrac{\sigma_v^2}{(2M+1)^2}}{\sigma_f^2+\sigma_v^2} & n_1=n_2=0\\ \dfrac{\dfrac{\sigma_v^2}{(2M+1)^2}}{\sigma_f^2+\sigma_v^2}, & -M\le n_1, n_2\le M, \text{ except } n_1=n_2=0\\ 0, & \text{Otherwise}\end{cases} \quad (9)$$

After finding estimation of watermark, get only one watermark from repeated watermark with folding operation. Performing the correlation operation between the watermark and Hadamard matrix, we can get the detection result.

Steps of detection are performed as following;

1) Find α value of $g(n_1, n_2)$ in the same way as embedding steps.
2) Estimate $P_v(w_1, w_2)$ with α.
3) Wiener filter is estimated with $P_f(w_1, w_2)$ and $P_v(w_1, w_2)$ by Eq. (7). From this estimation it can estimate the noise signal.
4) Divide noise signal with α by Eq. (2) and find the watermark using correlation operation with Hadamard matrix.

4. EXPERIMENTAL RESULTS

In experiment, we used 5169 × 1262 sizes of X-ray images with 16-bit resolution. Instead of using the raw material, we converted the images into 8-bit gray images without changing the spatial resolution. We used blind watermark detection approach which does not require any original image during detection process and 128, 512, and 1024 Hadamard matrix which have good correlation characteristics. In such cases, we use the Hadamard matrix for watermark and each column expresses as one symbol. We select 8 symbols randomly and the Hadamard matrix size is changed for each test (128×128, 512×512 and 1024×1024). Watermark is created to repeat same size with embedding area.

In this paper, we focused on robust watermarking against JPEG compression, in which the consideration of JPEG compression about watermarking attack is sufficient because X-ray images from container inspection is well managed and other malicious attack is difficult in current custom system. Just JPEG compression is inevitable natural processing for saving the significant amount of image data and sending it. We considered re-inspection of watermarked X-ray images, so we don't embed watermarks into the area of container box, but embed watermarks into truck area. Fig. 4 shows an original X-ray inspection image and Fig. 5 an area of truck in X-ray image for watermark embedding.

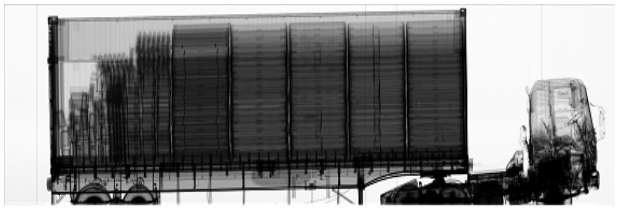

Fig. 4 X-ray inspection image of container truck (BMP format, 5169 × 1262 size, 19,574,784 Bytes)

Fig. 5 Truck area of X-ray image for watermark embedding (196 × 4677 size)

At first, we embedded 8 × 7 bit information with 128 Hadamard matrix, which can express unique 7 bits of user information. In watermark detection process, we used folding method for all minimum watermark segments to increase the detection ratio of watermark. Sequentially, we did experiment with 8 × 9 bit information with 512 Hadamard matrix which can express unique 9 bits of user information, and 8 × 1024 bit information with 1024 Hadamard matrix which can express unique 10 bits of payloads. We did check imperceptibility of watermarked images from JPEG compression in which Quality 90 ~ Quality 30. The Quality means picture quality of JPEG decoded image.

Fig. 6 shows an enlarged part of original image, Figs. 7 ~ 9 show an enlarged part of watermarked images for payload length. Using longer payload means that it is embedded more data. Images between Quality 90 and Quality 30 have a little difference with original image. Hence, the X-ray image in inspection system may use JPEG compression at Quality 30.

Fig. 6 An enlarged part of original image

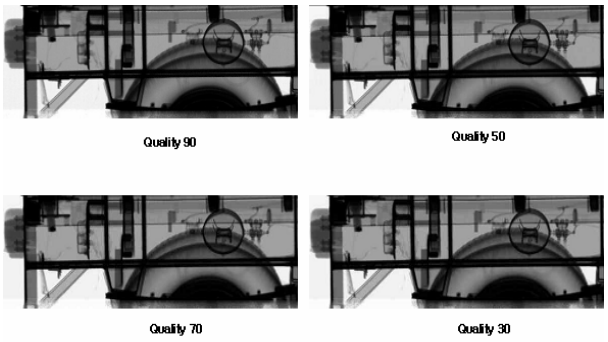

Fig. 7 Compressed image with 128 watermark matrix

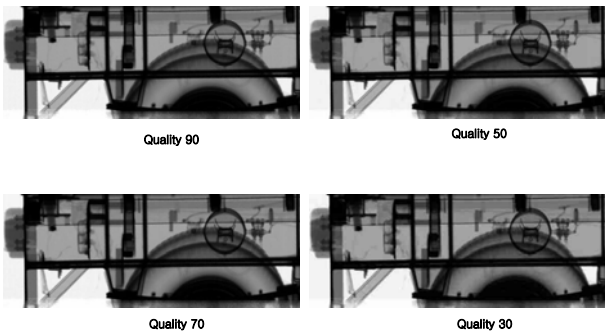

Fig. 8 Compressed image with 512 watermark matrix

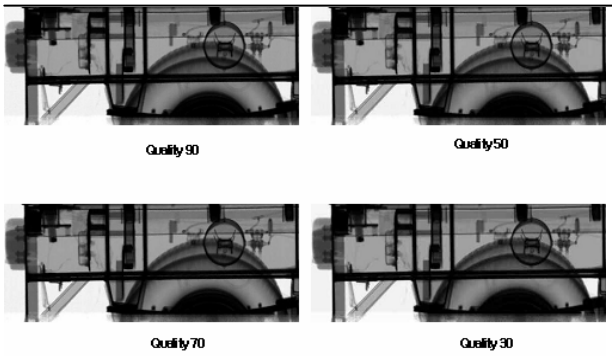

Fig. 9 Compressed image with 1024 watermark matrix

Table 1 ~ 2 show detection ratio after JPEG compression with permutation and without permutation. We performed each test 10 times. In Table 1, it shows that from quality 80, detection ratio begin to down with 128 length. Between 90 Quality and 50 Quality, the longer payload it has, the higher detection ratio it has. In Table 2, it shows detection ratio with permutation. The results are decently high detection ratio. Regardless of payload length, Until Quality 20, all watermarks were detected.

As a result of experiment, we find that the information can be embedded to X-ray image without large degradation of image quality. Proposed algorithm has a robustness of JPEG compression and has high detection ratio with permutation.

Table 1 Watermark detection ratio for various watermark matrix and compression attacks without permutation.

length / quality	128	512	1024
90	10	10	10
80	9	10	10
70	8	8	10
50	2	6	8
30	2	1	0
20	1	0	0
15	0	0	0

Table 2 Watermark detection ratio for various watermark matrix and compression attacks with permutation.

length / quality	128	512	1024
90	10	10	10
80	10	10	10
70	10	10	10
50	10	10	10
30	10	10	10
20	10	10	10
15	6	5	5

5. CONCLUSION

In this paper, authentication technologies for X-ray inspection images in container merchandises were introduced and a method of authentication for X-ray inspection images was proposed. Until now, X-ray images of container merchandises have been managed without any authentication of inspection results and environments, it means that there was no any action for protection of illegal copy and counterfeiting of X-ray images as inspection results. Our proposed algorithm indicates to put important information about X-ray inspection results on an X-ray image without affecting the original image. Therefore, this paper will be useful in determining an appropriate technology and system specification for authentication of X-ray inspection images.

As a result of experiment, we find that the information can be embedded to X-ray image without large degradation of image quality. Actually, because X-ray inspection images in container merchandises have much larger size than other image, JPEG compression is necessary. Our proposed algorithm has high detection ratio in attack of JPEG compression in Quality 20 and we cannot recognize visual difference between compressed image in Quality 30 and image in no compression. The algorithm was applied for a part of X-ray image but if we combine it with image automatic-recognition technology, more variable and much more information can be embed.

REFERENCES

[1] S. Katzenbeisser, S. and F. Petitcolas, “Information Hiding techniques for steganography and digital watermarking,” *Press of Artech House*, 2000.

[2] N. Johnson, Z. Duric, and S. Jajodia, “Information Hiding techniques for steganography and digital watermarking –Attacks and Countermeasures,” *Press of Kalwer Academic*, 2001.

[3] I. Cox, M. Miller, and J. Bloom, “Digital Watermarking,” *Press of Morgan Faukmann*, 2002.

[4] J. Pan, H. Huang, and L. Jain, “Intelligent watermarking techniques,” Press of World scientific, 2004.

[5] Hae Yong Kim and Amir Afif, “Secure authentication Watermarking for Binary Images,” *Computer Graphics and Image Processing,* 2003.

[6] D. Vleeschouwer, C. Delaigle, and B. Macq, “Invisibility and application functionalities in perceptual watermarking—an overview,” *IEEE Proceedings*, vol. 90, pp. 64-77, 2002.

[7] A. Tefas and I. Pitas, “Robust spatial image watermarking using progressive detection,” *Proc. IEEE ICASSP*, 2001.

[8] P, Shlichta, “Higher-dimensional Hadamard matrices,” *Information Theory on IEEE Transactions*, 1979.

[9] Ioannis Pitas, *Digital image processing algorithms*, Prentice Hall International (UK) Ltd*,* 1993.

[10] J. S. Lim, *Two-Dimensional Signal and Image Processing*, Prentice Hall, 1990.

ACKNOWLEDGEMENT

This work has been partially supported by "Research Center for Future Logistics Information Technology" hosted by the Ministry of Education, “RIS” by KOTEF.