A Robust Public-key Watermarking Algorithm Based on Contourlet Transform and its Application

Yanjun Hu, Guanjun Wang, Xinde Cao, Lei Yang
School of Information & Electronic Engineering, China University of Mining and Technology,
221008, XuZhou, Jiangsu, P.R.China
Email: {yjhu, wgjcumt, xindecao, leiyang}@cumt.edu.cn

Abstract— **This paper proposed a robust public-key watermarking algorithm based on contourlet transform and its application in coal mining information construction combining the practice. A solution scheme combining the robust watermarking technology and Hash algorithm was proposed to meet the robustness and security requirements of the Electric Equipment Operation Tickets (EEOT). The scheme used the certification information which generated by Hash algorithm, and it was embedded into its image using robust public-key digital watermarking algorithm, so the EEOT contents can be double authenticated. Hash algorithm adopted the MD5 algorithm. The solution scheme was discussed in detail. After the contourlet transform and watermark signal were introduced, the watermark embedment and authentication processes were shown. Maximum capacity of watermarking algorithm was calculated that showed hash value can be hidden in. Experiments were done also shown that the watermarking algorithm is robust against common signal process. Key codes were shown in appendix. Finally, the conclusion was given.**

Index Terms— **watermarking, robust, public-key, application**

I. INTRODUCTION

Recently, building digital coal mine enterprise is carried out by many coal mining enterprises of China since it can improve the level of management and decrease accident rate [1] . And the traditional paper-based documents trans formed electronic documents. Meanwhile, some challenges emerge. One of those is how to ensure the electronic documents security. Encryption technology can not satisfy the requirement, while the robust public-key watermarking technology meets the requirement.

A public-key watermarking scheme is a watermarking system that do not require the original content and private keys in the watermark detection process[2]. Another character of public-key watermarking is that the algorithm detail can be published, so it is easily accepted by the mining enterprises users since they can know how it work. Hartung and Girod's paper[3] is the first paper to introduce the notion of the public-key(asymmetric) watermarking [4]. It is well understood that the public-key watermarking scheme can be more effective to against the attacks. Some public-key (asymmetric) watermarking schemes have been proposed, such as [5] and [6].

The goal of this paper is to propose a scheme that can confirm the security and reliability of important materials based on the robust watermarking technology which is used in practice. Firstly, the requirement description and analysis are given in Section II, and the solution scheme was proposed in Section III. In Section IV, the solution scheme based on watermarking technology was proposed in detail and result are given in Section V. The scheme discussed in Section VI. Finally, conclusion was given in Section VII.

II. REQUIREMENT DESCRIPTION AND ANALYSIS

Pingmei Corporation Electricity Works Plant (PCEWP) is in charge of power supply of Pingdingshan Mining Group. In order to improve the management level, an Intranet covers 15 substations which distribute at a radius of 15 kilometers area and an information management system building are carried out in PCEWP. In the ma- nagement information system, an EEOT management sub-system is needed. Because of the EEOT is an important document which would be filled in many scattered places, the EEOT is not only preserved in the database, but also is saved in paper-form, as well as an archive file after signing at the corresponding site from a management perspective. The problem that facing now is how to achieve effectiveness of the signature and UN-forget ability of the EEOT after the realization of electronic signature.

The signature and audit on the EEOT are operated by different people at different times or different locations, so the EEOT electronic signatures are relatively easy to modify and counterfeit at the circumstance of Network Office. This raised the following requirements for the function of audit signature:

- Invoicing job must be strictly carried out in accordance with the flow. Authorized users must enter the correct user names and passwords before auditing the contents of the ticket. Show the auditors pre-acquisition handwriting on the ticket after the approval of the contents by auditor.

doi:10.4304/jsw.6.11.2247-2254

• The printing measures must be secure to ensure that the user altered, forged invalid.

The most difficult task is how to achieve the final print of the paper-form EEOT which has secure measures. It is printed with the contents and digital signature authentication information, in order to ensure integrity and un-forget ability of the paper ticket. If no protective measure

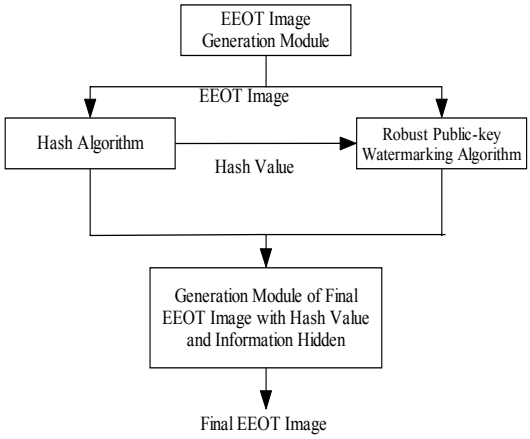

Figure 1. Solution scheme diagram

is used in EEOT, a fake EEOT could be generated with the help of Photoshop or other software.

If cryptography technology is used to protect EEOT, the following programs may be adopted:

• Calculate the check value of all the information on the ticket by Hash algorithm, and then print the check value on the paper ticket as additional information.

• Calculate the check value of the paper ticket and compare it with the check value on the EEOT, in order to judge whether the contents have been tampered. It is said that the information has not been modified if the two values are equal, otherwise, the information would have been altered.

However, such programs do not have the robustness. Once any part of the check value of the paper ticket calculated by hash algorithm is contaminated, verification will fail. So a solution scheme combining the robust watermarking technology and Hash algorithm will be discussed in next Section.

III. SOLUTION SCHEM E

The reason for the failure of above program is that its robustness is not strong. Therefore, a designed scheme is shown in Fig.1. In EEOT management subsystem, EEOT is generated as an image file. The file is calculated by Hash algorithm and a hash value used as check value is obtained. Then the check value is embedded into image. Printed check value and image with hidden information on the ticket in paper-form would realize the double signature". This is more subtle, but also more secure.

There is similar scheme proposed[7]. However, the authors only propose some minds about inserting the watermarking signature into the image, but do not introduce its principles either how to implement in [7].

The MD5 hash algorithm (Message-Digest Algorithm 5) was adopted. It was invented by professor Rivets in 1991. An algorithm based on the vulnerability of MD5 algorithm is invented in [8]. Though, it can find the data of same fingerprint and different plaintext in a very short time [9], the contents of the other same fingerprint data which is found by collision method is not determinate. If the method does not use the special data to forge the signature, there is not loss of safety problem [10]. So, MD5 algorithm is safe in this application situation.

IV. SOLUTION IMPLEM ENTION

There are two key parties in this solution. a) how to implement the hash algorithm, b) how to design a robust public-key watermarking algorithm.

Since this solution is implemented in Windows 2003 platform, functions provided by Microsoft .NET framework is used. Therefore, calculating the hash value of source data can use System. Security. Cryptography class of Microsoft .NET framework. Codes of hash value calculation are shown in appendix. So, this section mainly discusses the robust public-key watermarking algorithm that based on contourlet transform used in solution.

A. Contourlet Transform

Contourlet transform is also named PDFB (pyramidal direction filter bank); it is a new extension of the wavelet transform with multi-resolution, local orientation, multi-directional and neighbor sector, such as sampling and anisotropic nature. Its basis function is found in multi-scale and multi-up, a few coefficients can be effectively catching the image edges, while the edges are a natural image of the main features.

Contour transform firstly use a similar multi-scale wavelet decomposition of catching singular points, and then under the direction of information will be located closing to the singular points so as to marshal a contour segment. Laplace decomposition decomposed the original image into low-frequency sub-band and high frequency sub-band. The low-frequency sub-band is generated by the original image through the two- dimensional low-pass filtering and de-interlacing every other line sampling; after the sampling and low-pass filter, the low-frequency sub-band will form the same low-frequency components with the original image size, the original image minus the low-frequency components to create high-frequency sub-band. After another direc- tion for high-frequency sub-band filter bank is decom- posed into 20 sub-band direction. Repeating the above process on the low-frequency sub-band can achieve multi-directional multi-resolution decomposition [11].

Contour transform is applied to describe the reason for the natural images because the natural images of objects in the direction of information and texture information can effectively be expressed by contour-wave domain's basis function and also can be rapidly approached [12]. Compared to the critical sampling wavelet, LP decompo-

sition of each floor in high-dimensional cases, produced only a band pass image, so as to avoid scrambling phenomenal [11] .

Two-dimensional direction filter (Directional Filter Bank, DFB) applied to LP decomposition of high frequency components at every level, in any scale can be broken down to be 2*n* direction of sub-band. LP and the DFB with the formation of double-layer filter group is known as the pyramid structure, the direction of filter PDFB, essentially due to PDFB approximation is based on the manner in paragraph outline of the original image, It is also known as discrete wavelet transform contour [11].

Fig.2 shows an example of contourlet transform.

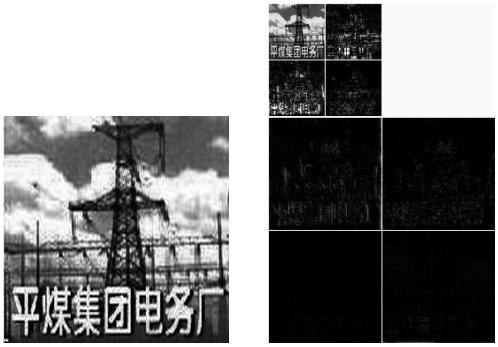

Figure 2. Original image and its contourlet coefficients

B. Watermark Signal

In [13], a generation method of optimal sine pseudo-random sequences (OPSS) is proposed. If p is a prime number and b is the primitive root of p, ni is obtained by

$$n_i = p = < 0. \overset{\bullet}{a_i} \ldots a_{p-1} a_1 \ldots \overset{\bullet}{a_{i-1}} > \quad (1)$$

Where $i = 1 \sim p - 1$. Furthermore, optimal sine pseudo random sequences $OPSS(p)$ is obtained.

$$OPSS(p) = \{\sin(2\pi ni/p \mid i = 1, 2, \cdots, p-1\} \quad (2)$$

The $OPSS(p)$ has good pseudorandom character which is proved. However, it can not be directly used as watermark signal. So, we proposed a generation method of extend optimal sine pseudorandom sequences (EOPSS) in [14]. EOPSS is obtained by inserting a random real data I ($I \ll p$) after the $k-$th$(1 \le k \le p)$ data of $OPSS(p)$.The EOPSS signal is denoted as $EOPSS(k, OPSS(p))$ [1] .

Let a sequence $X = EOPSS(k, OPSS(p))$, extending the sequence X with the period $p + 1$, the auto- correlation function of X is:

$$Co(\tau) = \frac{1}{p}\sum_{i=1}^{p} x_i x_{i+\tau}$$

$$\approx \begin{cases} 0.5 & ;\tau = 0 \\ -0.25 & ;\tau = \frac{p}{2}, \frac{p}{2}+1 \\ 0 & ;0 < \tau < p-1; \tau \neq \frac{p}{2}, \frac{p}{2}+1 \end{cases} \quad (3)$$

Here, $i + \tau$ *means* $i + \tau$ (mod p). The auto-correlation character was also proved.

Finally, a watermark signal $W(p, sp, st, and\ j)$ which can be used in a robust public-key watermarking algorithm can be generated by

$$W(p, sp, st, m) = \sum_{j=1}^{m} EOPSS(ip_j, OPSS(p)) \quad (4)$$

where $ipj = (sp + j \cdot st) \bmod p$. And, m, st, sp $(0 \le sp \le q - 1)$ are generation parameters. If $m \le p/10$, $st \approx p/10$ extending the sequence $W(p, sp, st, j)$ with the period $p + 1$, the auto-correlation function of $W(p, sp, st, j)$ is

$$Co_{W,W}(\tau) \approx \begin{cases} 0.5m & \tau = 0 \\ -0.25m & \tau = \frac{p-1}{2}, \tau = \frac{p+1}{2} \\ 0 & else \end{cases} \quad (5)$$

Experiments done by [14] shows that the watermark-maker should avoid using $m = 1$. The attackers can obtain the p; because p value is the sequence length subtracts 1. The attackers can construct a serial signals $W(p, i, 0, 1)$.After the values of $CoW(p,i,0,1), Pk(\tau)(i = 0, 1, \cdots p-1)$ are calculated, the minimum value can be obtained.Suppose the $k-$th element of $CoW(p,i,0,1), P_k(\tau)(i = 0, 1, \cdots p-1)$ is minimum value. The correct sp value is k. Experiment shown in Fig.3 is done. The valley of $CoW(p,i,0,1), Pk(\tau)(i = 0, 1, \cdots p-1)$indicates the correct value used in watermark. If $m > 1$, since the $m, st, and\ sp$ are interactional, the attackers can not get the value of m, st, sp. Fig.4 shows that although the correct m is used, the minimum value does not point to the correct sp *because* of the wrong st. That is the reason that a watermark is compounded by several EOPSS instead of using EOPSS directly.

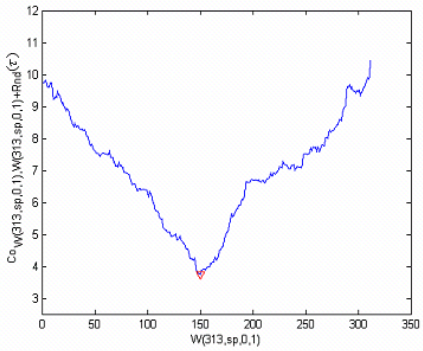

Figure 3. experimentation of getting private key sp by calculating all of possible watermark, the minimum value of $CoW(313;150;0;1)$; $W(313;sp;0;1)+Rnd(\tau)$ indicates the correct sp value, as ∇ marked in figure

C. solution Scheme

[1]The value of I has trivial effect on the correlation characteristic of sequence while $I \ll p$, which always happens in practice. The most important parameters are parameter k and p. So I is omitted from the symbol denoted EOPSS.

The solution scheme consist three processes, a) watermark signal generation process in which MD5 value is coded watermark signal, b) EEOT generation process, c) EEOT authentication process used to judge a disputative EEOT.

1) Generation of Watermark Signal: The information hidden in EEOT is MD5 value of EEOT image. However, the MD5 value can not be directly inserted into the image that is shown in Fig.1. The MD5 value must be coded watermark signal. The following description shows how to generate the watermark signal by using MD5 value.

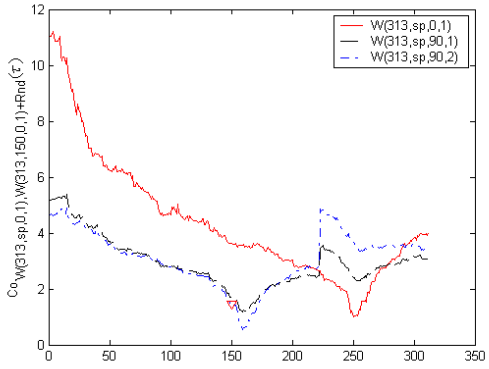

Figure 4. experimentation of trying to find the correct *sp*. It shows that if the *st* is wrong, whether *m* is correct or not, the minimum value of ε did not indicate the correct *sp* value, as ∇ marked in figure

Step1: Generate the original image of the EEOT, store it
with JPG format, then calculate the 32 character elements of MD5 denoted as $\{ch1, ch2, \cdots, ch32\}$.

Step2: Choose a p, and then generate an $OP\ SS\ (p)$

Step3: Divide MD5 value $ch1, ch2, \cdots, ch32$ into k groups. Every group has m *character* elements of MD5.

Step4: The watermark signal is generated by

$$W(p,sp,st,m)=\sum_{j=0}^{m} EOPSS(ip_j, OPSS(p)) \tag{6}$$

the values of $k = 1; 2; \cdots$; *msp*, *st* and data inserted are random generated by using Random object of C# object

It is considered as private key which must not be Published that how to divide MD5 value into groups. It means k and m must keep secret since they are private keys.

The Random object in.NET platform object libaray has a character that the same paramater is used when call the construction function the same random value will output. It means that the random data can be reappeared. So, the watermark embedded can be regenertate that is just needed
by the solution.

2) Generation of EEOT: After transforming the MD5 value to the corresponding pseudorandom signal sequence $Wk(p; sp; st; m)$, it is considered as private key in watermarking algorithm and is embeded into a image.

Step1:Generate a random sequence *S*rnd .The elements of *S*rnd are normally distributed with mean 0,variance $\sigma 2 = 1$.

Step2: Create a public key *S*pub by

$$Spub = Wk + Srnd \tag{7}$$

where m is one of the parameter which is used to create watermark signal $Wk\ (p, sp, st, m)$.

Step3: Perform contourlet transform on original image *C*o , and a coefficient sequences *S*o is obtained.

Step4: Choose an α, then embed watermark *S*wn based the following equation:

$$Sw = So + \alpha Wk \tag{8}$$

Step5: Replace the *S*o by *S*w , and reconstruct image,then the watermarked image *C*w is obtained.

Step6: Calculate the value of v = PSNR(*C*w , *C*o) , if $v < 40$, re-choose a α value, and step5-step6 are repeated until the $v > 40$.

3) EEOT Authentication: This process is used to distinguish the contents of EEOT. So, in this process, the origianl image can be re-generated.

Step1: With the help of special system to generate the original image of the implementary EEOT, store it with JPG format, and calculate MD5 value of the image.

Step2: If the calculated MD5 value and the MD5 value printed on EEOT are inconsistent, it is not a normal ticket. Ending the process.

Step3: Transform the MD5 value to the corresponding pseudorandom signal sequence $Wk\ (p, sp, st, m)$.

Step4: Let *C*n denote the image printed in EEOT to be detected. Perform contourlet transform on image *C*n as it is described in the step3 of watermark generation of EEOT process, and a sequences *S*n is obtained.

Step5:Calculate the auto-correlation function Co(*S*n,*Wk*). A value ε of likelihood function is obtained.

$$\varepsilon = L(C\ o(Sn\ ,\ Wk\ ),\ Bs(p,\ \tau\ )) \tag{9}$$

where $Bs(p, \tau)$ is defined

$$Bs(p,\tau)=\begin{cases} 0.5; & \tau=0 \\ -0.25; & \tau=\frac{p}{2},\frac{p}{2}+1 \\ 0; & 0<\tau<p-1;\tau\neq\frac{p}{2},\frac{p}{2}+1 \end{cases} \tag{10}$$

and function $L(X, Y)$ is defined

$$L(X,Y)=\sum_{n=0}^{len-1}\left|\frac{X(n)-X_m}{2|X(0)-X_m|}-\frac{Y(n)-Y_m}{2|Y(0)-Y_m|}\right| \tag{11}$$

(*Xm* and *Ym* is mean of X and Y , *len* is the length of sequence X and Y).

A threshold d is choosen. If $\varepsilon > d$, the *C*n is a fake EEOT, the process is terminated .

Step6: Erase the watermark based on the following equation:

$$Sn = Sn - \alpha Wk \tag{12}$$

Step7:Replace the *S*n by *S*′n, and reconstruct an image *C*e.

Step8: Evaluate the image *C*e. If *PSNR*(*Ce;Cn*) >40, consider *C*n is a normal EEOT.

D. Maximum Capacity of Watermarking

As it can be seen from the scheme description, the MD5 value is hidden in the image through robust public-

key watermarking. The maximum capacity of watermarking determine whether hash value can be hidden in or not.

From description of watermarking algorithm, the algorithm model are shown as Fig.5. There are two channels, a) the channel information coding and b) transmission channels.

1) Information coding channel capacity: Information encoded channel input is hidden information, the channel's output is watermark signal embedded into the

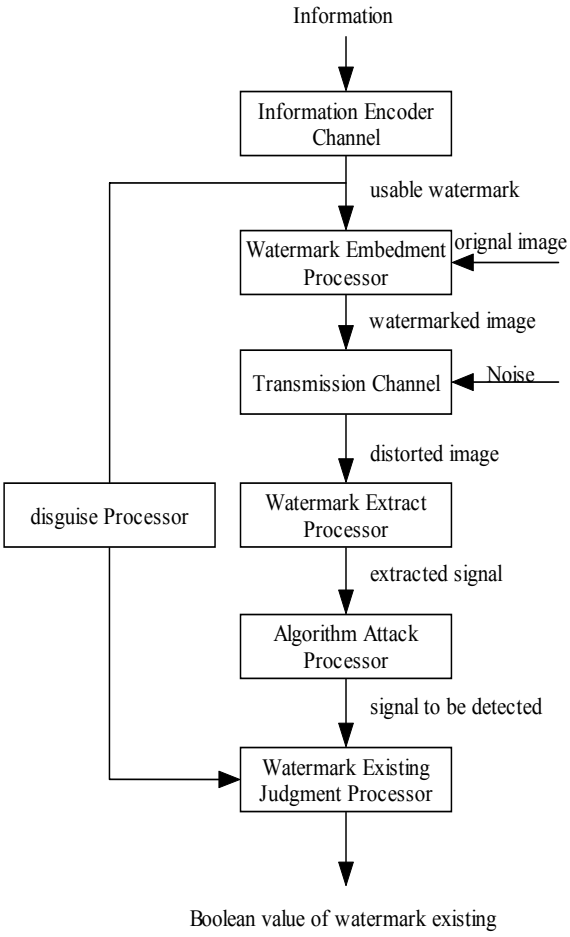

Figure 5. Public-Key Watermarking Model

image, the channel is a virtual channel, let S_{info} for a collection of information to be hidden, let *S*uw for the watermark signal can be set, then the information encoding channel capacity denoted as C_{incode} is maximum mutual information of *S*info and *S*uw ,

$$C_{\text{incode}} = \max_{p(S_i^{uw})} I(S^{\text{info}}, S^{uw}) = H(S^{uw}) - H(S^{uw} \mid S^{\text{info}}) \tag{13}$$

Taking into account the practical significance of watermarking algorithm, this channel is a discrete noiseless channel, that is

$$P(S_i^{\inf o} \mid S_j^{uw}) = \begin{cases} 1, & \text{if } S_j^{uw} \text{ is coded by } S_i^{\inf o} \\ 0, & \text{others} \end{cases} \tag{14}$$

Thus

$$C\text{incode} = H(S\text{uw}) \tag{15}$$

2) Transmission channel capacity: Transmission channel input is image with watermark, the output is tested watermark image (and to test whether there is the process of the watermark signal input). Let *S*wi denote channel input symbols, let *S*dis denote a set of channel output symbols, and assume that the transmission process is described conditional probability $p(S\text{noise} \mid S\text{wi})$ between the attacks (noise) and the input signal.

In the case of a fixed original image, the image with watermark is created by the watermark signal which can be used , that is,

$$p(S\text{wi}) = p(S\text{uw}) \tag{16}$$

$$p(S_{\text{j=i}}^{\text{noise}} \mid S_{\text{i}}^{\text{wi}}) = p(S_{\text{j=i}}^{\text{noise}} \mid S_{\text{i}}^{\text{uw}}) \tag{17}$$

As the watermark embedding process employs the signal is that in time-space-mode added, taking in all the image pixel value range is limited, so you can get

$$P(S_{\text{j}}^{\text{dis}} \mid S_{\text{i}}^{\text{wi}}) = P(S_{\text{j=i}}^{\text{noise}} \mid S_{\text{i}}^{\text{uw}}) \tag{18}$$

Therefore, the availability of the probability of channel output symbols

$$P(S_{\text{j}}^{\text{dis}}) = \sum_k p(S_{\text{k}}^{\text{wi}}) p(S_{\text{j=k}}^{\text{noise}}) \tag{19}$$

Through the Eq.16 Eq.19, the available input and output variables of the mutual information

$$I(S^{wi}, S^{dis}) = \sum_i \sum_j p(S_{\text{i}}^{\text{wi}}, S_{\text{j}}^{\text{dis}}) \log \frac{p(S_{\text{i}}^{\text{wi}}, S_{\text{j}}^{\text{dis}})}{p(S_{\text{i}}^{\text{wi}}) p(S_{\text{j}}^{\text{dis}})} \tag{20}$$

Therefore, this channel capacity $C_{p(S_{j=i}^{noise} \mid S_i^{wi})}$

$$C_{p(S_{\text{j=i}}^{\text{noise}} \mid S_{\text{i}}^{\text{wi}})} = \max_{p(S_{\text{i}}^{\text{uw}})} I(S^{\text{wi}}, S^{\text{dis}}) \tag{21}$$

Consider the algorithm must be able to withstand all the attacks, then the transmission channel capacity is defined as

$$C_{trans} = \min_{p(T^{airs} \mid T^{wi})} C_{p(S_{j=i}^{noise} \mid S_i^{wi})} \tag{22}$$

3) Channel capacity: The algorithm capacity is defined as the minimum capacity of two channels, according to Eq.15 and Eq.22, algorithms capacity available

$$C_{\text{trans}} = \min_{p(T^{\text{airs}} \mid T^{\text{wi}})} C_{p(S_{\text{j=i}}^{\text{noise}} \mid S_{\text{i}}^{\text{wi}})} \tag{23}$$

of which

$$C_{p(S_{\text{j=i}}^{\text{noise}} \mid S_{\text{i}}^{\text{wi}})} = \max_{p(S_{\text{i}}^{\text{uw}})} \sum_i \sum_j p(S_{\text{i}}^{\text{uw}}) \bullet p(S_{\text{j=i}}^{\text{noise}} \mid S_{\text{i}}^{\text{uw}}) \log \frac{p(S_{\text{j=i}}^{\text{noise}} \mid S_{\text{i}}^{\text{uw}})}{\sum_k p(S_{\text{k}}^{\text{wi}}) p(S_{\text{j=k}}^{\text{noise}})} \tag{24}$$

As the channel capacity is a convex function of $P\left(S_{j=i}^{noise} \mid S_i^{wi}\right)$, noises (attackers signals) have a greater impact on channel capacity.

4) Capacity limit: As can be seen from the Eq.23 and Eq.24, when the $p(S_{j=i}^{noise} \mid S_i^{wi}) = 1$, the channel capacity $C\max = H(S\mathrm{uw})$, is available watermark signal entropy, according to the maximum entropy theorem for discrete source, when the watermark signal can be used to take such estimates the distribution of maximum entropy, the algorithm of the maximum capacity.

$$C\max = H(S\mathrm{uw}) = \log \mid S^{\mathrm{uw}} \mid \tag{25}$$

Where $\mid S^{\mathrm{uw}} \mid$ is the number of available of watermark signal.

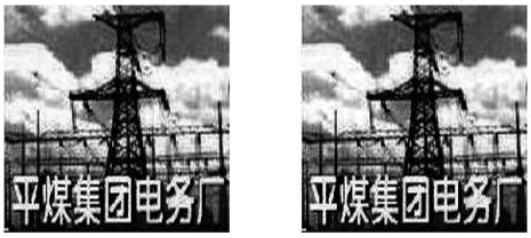

Figure 6. Original image and watermarked image

Furthermore, according to PSNR definition,

$$PSNR = 10\lg[MN\left(S_{\max}^{\mathrm{ori}}\right)^2 / \sum_{i,j}\left(S_{\mathrm{i,j}}^{\mathrm{uw}}\right)^2 / 10^{\mathrm{d}/10}] \tag{26}$$

Let distortion threshold is d, Eq.25 can be converted as

$$\sum_{i,j}(S_{\mathrm{i,j}}^{\mathrm{uw}})^2 < MN(S_{\max}^{\mathrm{ori}})^2 / 10^{\mathrm{d}/10} \tag{27}$$

Assumptions the watermark is Wk (p, sp, st, m) and embedment amplitude is α, Eq.27 can be turned into,

$$\alpha < \sqrt{\left(S_{\max}^{\mathrm{ori}}\right)^2 / 10^{\mathrm{d}/10} / m\sum_{i}^{p}\sin^2\left(2\pi \mathrm{n_i} / p\right)} \tag{28}$$

The image printed on EEOT is shown in Fig.6 $S^{\mathrm{ori}} = 255$, $\alpha < 0.013$ by Eq.27. If $p = 17$, $m = 3$, the capacity limit of would be 139 bit. So the MD5 value can be hidden in this image.

Calculation was found that although the image size does not directly affect the watermark amplitude range available. But, more larger images more greater the range of p, sp, st, m while W_k (p, sp, st, m) is generated. So, there is always existing a image can contain the MD5 value.

E. Robustness of algorithm

1) Watermark effect on vision: Let $p = 313$, $m = 3$, $\alpha = 0.013$, sp and st are random value. Fig.6 shows the experiment result of watermark effect on vision. The left image is the original image and the right one is the watermarked image. The watermarked image is as the same as original image on vision. It is calculated that PSNR value is 40.3042dB and ε value is 22.9828.

2) Common signal process effect on watermark detection: Common signal process is carried on watermarked image, $\varepsilon 1$ value in Table I show the detection result. In Table I , $\varepsilon 2$ value are results of algorithm based wavelet which use the same watermark signal and same embedment intensity. It also shown that the watermarking algorithm is more robust than the watermarking algorithm based on wavelet transform. But, Table II shows that the watermarking algorithm based on wavelet transform is more robust than the watermarking algorithm. It is expected because that JPEG stand is based on the wavelet transform. The results show that the algorithm is robust against common signal process.

TABLE I.
COMMON SIGNAL PROCESS EFFECT ON WATERMARK DETECTION

Operation	$\varepsilon 1$	$\varepsilon 2$
watermarked image is added random noise with mean 0 and maximum 0.1	30. 2519	37. 5096
watermarked image is added Gauss noise with mean 0 and variance 0.02	34.6327	42.4339
watermarked image is fuzzed	73.7519	98. 5512
watermarked image with median filter used	32. 5698	43. 2333
watermarked image with Wiener filter used	39.7065	48.4908

TABLE II.
ROBUSTNESS TO JPEG COM PRESS

quality	$\varepsilon 1$	$\varepsilon 2$
10	52.9660	42.1624
20	49.1841	38.8165
30	45.8003	37.8372
40	40.7275	37.3633
50	38.7065	36.5558
70	36.0684	35.7318

V. SCHEME IMPLEMENTATION RESULT

The scheme was built on the .NET platform, and the GDI+ technology was used. The scheme was implemented in B/S module. Windows 2003 was installed in server computer and IIS was used as web server.

Fig.7 and Fig.8 are the scene shots. Fig.7 is the EEOT without any authentication information, Fig.8 is the EEOT containing certification information.

Compare with Fig.7 and Fig.8, there are two difference:

•MD5 value was added on the upper left corner.

•Image with corresponding information was inserted in the remarks column.

VI. SCHEME DISCUSSION

A. Robustness and Security of Scheme

The program as a whole is robust and safe.

From the implementation of the program, it can be concluded that the program's core is the realization of signal which is embedded by watermarking algorithm. Except that, program is also needed to calculate MD5 value of the original image, and generate the EOPSS sequence by the value.

Therefore, to the resistance of algorithm attack of this program, the algorithm is safe.

1) the MD5 value of the original image is public, an attacker cannot restore from the MD5 value of the corresponding original image, this is guaranted by the corresponding MD5 algorithm.

2) attacker cannot get the watermark signal embedded in the image generated by the MD5 value, it is unable to restore the value of the MD5 by EOPSS, since the attacker does not know the private key. This is guaranted by watermarking algorithm.

The algorithm robustness is concerned, it can resist general digital signal processing attacks. The steps of calculate MD5 value and generate the EOPSS sequence do not affect its capability.

B. Lack of Scheme

Program has some inadequacies.

The anti-algorithm attack ability of this program is not perfect. Because embedded watermark image signal (composite EOPSS sequence) is generated by the MD5 value, and the method for the generation is public.

Attacker can use method of exhaustion to construct the embedded watermark signal to attack. The possibility of choosing m characters from 32 elements of MD5 characters array to generate EOPSS is

$$p_{\mathrm{m}}^{\mathrm{m}} \sum_{\mathrm{k}=0}^{\mathrm{m}}{}^{\overline{32}} C_{32-\mathrm{k}\bullet\mathrm{m}}^{\mathrm{m}} \tag{29}$$

that is attack intensity:

$$p_{\mathrm{m}}^{\mathrm{m}} \sum_{\mathrm{k}=0}^{\mathrm{m}}{}^{\overline{32}} C_{32-\mathrm{k}\bullet\mathrm{m}}^{\mathrm{m}} tobeadded \tag{30}$$

Therefore, it is best to not open the method which is used to generate EOPSS by MD5 values for safety considerations. This will be helpful for the ability of anti-algorithm attack.

It is relatively difficult to synchronize the images. Because the watermarking algorithm has very strict requirements about characters of the image, when detect the watermark signals on the paper image, the image border alignment must be accurated. In practice, it is more difficult to overcome this problem.

VII. CONCLUSION

This paper introduces the application of digital watermark technique in the coal mines information construction. From the instruction of situation and needs analysis of the EEOT integrity and robust security, we propose the scheme based on robust public-key digital watermarking algorithm, inserting the certification information is generated by Hash algorithm into the EEOT image. It is

Figure 7. Original Work Ticket Image

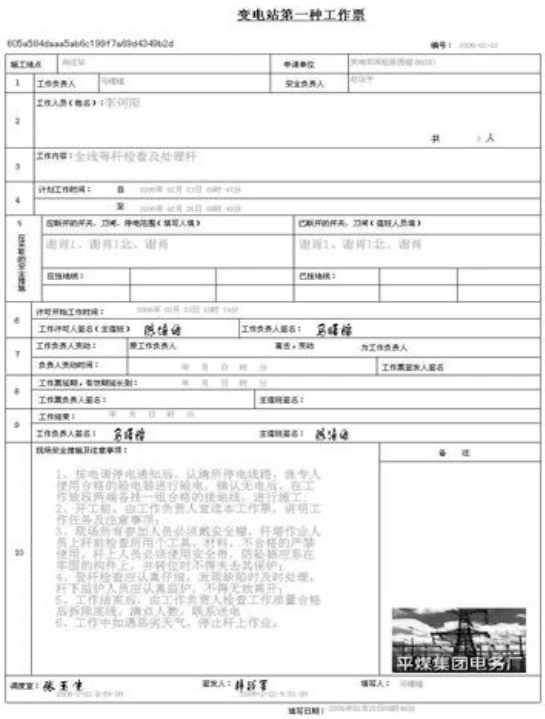

Figure 8. Watermarked Work Ticket Image

discussed the platform of the implementation and the key technologies. Practice shows that the program is feasible, but the program is very strict with the extraction of images, which often creates a bad influence. This scheme is not limited to the EEOT application, it can also be used at all the similar situations.

APPENDIX

A. Generation Watermarked Image

In ASP.Net applications, according to the following steps can dynamically generate a picture. Firstly, make the property of Response. ContentType as “image/jpeg”, so that the browser explain the response correctly. Secondly, do some corresponding operation on the GDI +. Lastly, the Save() method of Image object was used to output the watermarked image to the user’s browser.

```
//read the image file
Bitmap bitmap = new Bitmap(filename);
int imgWidth, imgHeight; imgWidth=bitmap. Width;
    imgHeight=bitmap. Height;
bitmap = new Bitmap(bitmap, imgWidth, imgHeight);

//creat the brush
Texture Brush my Brush = new Texture Brush (bitmap);
bitmap = new Bitmap(imgWidth, imgHeight);
Graphics g = Graphics. FromImage(bitmap);
g.Fill Rectangle (myBrush, 0, 0,imgWidth, imgHeight);
FontFamily fontFamily =new FontFamily("Arial");
Font font = new Font(fontFamily,12, FontStyle. Regular,
    GraphicsUnit.Pixel);

//draw the MD5 value g. DrawString(strMD5Val,font,
new SolidBrush (Color.Black), 97,
101);
//send the image to user’s  browser Response. ContentType
    = "image/jpeg"; Response. Clear(); bitmap. Save
    (Response. OutputStream, System. Drawing. Imaging.
    ImageFormat. Jpeg);
```

ACKNOWLEDGMENT

This work is supported by the Youth Foundation of China University of Mining and Technology, No.2008 A019.

REFERENCES

[1] Zhang Shen, Ding En-Jie, Zhao Xiao-Hu etc. Digital the China Coal Society,2007,32(9):997-1001

[2] Yong dong Wu, Feng Baom, Changsheng Xu. On the security of two public key watermarking schemes. Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia. Vol 2 , 2003, pp:975 -979

[3] Hartung F, Girod B. Fast public-key watermarking of compressed video. Proceedings of the IEEE International Conference on Image Processing (ICIP97). 1997. pp:528 531.

[4] Teddy Furon and Pierre Duhamel. An Asymmetric Watermarking Method ,IEEE Transactions on Signal Processing ,51(4), APRIL 2003, pp:981-995.

[5] J.Eggers, J.Su, and B. Girod, Public key watermarking by eigenvectors of linear transforms, Proc. Eur. Signal Process.Conf.Tampere,Finland,Sept.2000.Availabe:http: //www.lnt.de/eggers/texte/eusipco2000. pdf

[6] Yanjun Hu, Xiaoping Ma and Li Gao. A Robust Public-key Image Watermarking Scheme Based on Weakness Signal Detection Using Chaos System, Proc. International Conference on Cyberworlds, 2008, pp:477-480

[7] Assure Digital Home Page. 2007-05-13. http://www.assure digit.com

[8] Hancheng Liao. Image retrieval based on MD5. Advanced Computer Theory and Engineering International Conference, 2008,12:987-991.

[9] X.Wang. Collisions for Hash Functions Md4,Md5, Haval-128 and Ripemd.Crypto04.2004,Availabe: http://eprint.iacr.org/2004/199.pdf

[10] S.-J. Wang, H.-J. Ke, J.-H. Huang, et al. Concerns about Hash Cracking: Aftereffect on Authentication Procedures in Applications of Cyberspace. IEEE Aerospace and Electronic Systems Magazine. 2007, 22(1):354-359

[11] Yanling Li. De-nosing capability of a filter based on contourlet transform. Journal of Huazhong University of Science and Technology(Nature Science Edition). 2008, 36(8):28-30

[12] Do M. N, Nvetterli. M. The contourlet transform efficient birectional multi-resolution image representation, IEEE Transactions on Image Processing, 2005,14(12):2091-2106

[13] Dewen Hu. A novel generation mthods pseudo-random integer strings and pseudo-random sequence, Science in China(Series E), 2000, 20(3):258264

[14] Hu Yan-jun, Ma Xiao-ping, A novel watermark signal of public-key robust watermarking scheme,SETIT2005, 2005: 86

Yanjun Hu received his MS degree in communication and information system from Xuzhou, China University of Mining and Technology, P.R. China, in 2008. He is currently an associate professor at the China University of Mining and Technology. His research interests include digital watermarking and wireless sensor network.

Guanjun Wang received his bachelor degree in Electronic science and Technology from Huai Nan Normal University, in 2009.Now,he is studying in China University of Mining and technology.

Xinde Cao received his bachelor degree in Signal and Information Processing from Xuzhou Medical College, in 2009.Now,he is studying in China University of Mining and technology.

Lei Yang received his bachelor degree in Electronic Science and Technology from Chang Shu Institute of Technology, in 2009. Now, he is studying in China University of Mining and technology.