Research on the Dual Digital Watermark Algorithm Based on Information Hiding Technology

Wei Xian Li

Educational Technology Center, Lang Fang Teachers University, Langfang 065000, China

Abstract

In recent years, rapid development of the computer network technology promotes living quality of the people substantially, while the information security issues are increasingly prominent simultaneously, which causes the continuous increment of malicious information alteration and copyright infringement of the lawless persons. However, being as the important technology of protecting information security in the future, information hiding technology shoulders the important mission of safeguarding information security. By applying the information hiding technology in digital algorithm, one can solve information security issues effectively, promote the security in the links of information transmission, storage and reception, and ensure information reliability effectively. There are various digital watermark algorithms currently, while the function is relatively single, for it cannot give consideration to evaluation and index calculation of digital watermark simultaneously. Thus, it is necessary to study out a dual digital watermark algorithm with information hiding technology. For this purpose, this paper realizes embedding, extraction, detection and generation of digital watermark by utilizing information hiding technology, adopting various digital watermark algorithms, and fully combining with the relevant technological means.

Keywords: Information hiding technology, Dual digital watermark algorithm, Robustness, Semi-vulnerability.

1. RESEARCH BACKGROUND

1.1 Literature review

Along with coming of the information age, our life shows huge change, living quality is enhanced drastically, living standard is improved obviously, and the interpersonal communication becomes more convenient and various. However, following the use of such information tools as computer, the amount of information increases exponentially, which drives social development vastly. At the same time of continuous increment of the amount of information, such issues as malicious alteration and copyright infringement also show explosive increment, which directly reflects vulnerability of our country in information security currently. However, the development of science and technology makes the people beginning to strengthen information security further with relevant technological means, and information hiding technology and digital watermark technology emerge at the right moment. Many scholars also carry out the researches on digital watermark and information hiding technology, and some scholars encrypt the information by combining fingerprint verification with digital watermark and obtain favorable progress on the research achievements (Xie, 2006). Some scholars give watermark treatment to the digital images by utilizing the wavelet transform technology in information hiding technology and invent the digital image watermark algorithm thereby, this algorithm can realize copyright authentication and identification of digital image by applying wavelet transform in digital image, and it obtains favorable effects (Cheng and Wang, 2006). Some scholars give corresponding summary and sorting to the research achievements and progress of the digital watermark technology, and further identify significance of the digital watermark technology in information security (Jiang et al., 2006). Wang Yan et al give relevant improvement to the wavelet transform technology in information hiding technology, thus the wavelet transform technology shows even more excellent effect in information authentication and identification (Wang and Li, 2012). Some scholars give self-destructive digital watermark treatment to the communication information to further promote the confidentiality in information communication, and self-destruction of the communication information can be realized once there is some person eavesdropping communication or invading communication system, to prevent hackers from stealing and eavesdropping the secret information (Wang et al., 2017). Generally speaking, researches of the relevant scholars on information hiding technology and digital watermark are more and more
profund, and relevant scientific achievements begin to emerge constantly, which makes it much more difficult to steal and tamper the information by lawless persons.

1.2 Research purpose

Research purpose of this paper is to put forward the relevant improvement measures and implementation plans feasible in technology and establish the dual digital watermark algorithm considering index calculation and evaluation simultaneously, by fully combining the modern technological means, based on the research on multiple digital watermark algorithms in digital watermark technology field and by using the information hiding technology, so as to solve the problem of imperfect digital watermark evaluation and index calculation, realize embedding, extraction, generation and detection of digital watermark, and make relevant scholars able to set up a digital watermark system model satisfying information security demand according to this dual digital watermark algorithm (Zhang, 2016). By applying such various algorithms as HVS adaptive algorithm, LSB algorithm, DWT algorithm and DCT algorithm, one can ensure the higher feasibility of this dual digital watermark algorithm in technology, relieve the current much more serious information security issue hereby, and avoid information tampering and stealing of lawless persons technologically.

2. OVERVIEW OF THE INFORMATION HIDING TECHNOLOGY

2.1 principle of the information hiding technology

Information hiding technology is the technology that certain algorithm embedding method is used in hiding such secret information with application value as copyright, serial number and password in the massive carrier information to obtain corresponding hidden carrier, realize hiding of the secret information and make the outsiders not being able to see contents of the secret information. The common carriers mainly include image, video, character and voice, and the named embedding algorithm refers to the method of hiding information according to the information masking effect and the own space and time redundancies of information (Wang, 2008). After adopting information hiding technology, the invaders without authorization are hard to confirm existence of the secret information in hidden carrier and are harder to extract and tamper the secret information in massive information carriers, so information security can be strengthened. The receivers with authorization can detect and recover the secret information in hidden carrier via detector and by using the secret key after receiving hidden carrier. Information hiding technology and information encryption technology has some common points in basic ideas, and the difference lies in that information hiding technology does not restrict information sharing, storage and reading of others by information encryption but avoids information perception and destruction of others by hiding the information with information hiding technology. Moreover, information hiding technology can hide all of the information, so it cannot be perceived by others easily (Han and Zhu, 2008). Information encryption technology can restrict information acquisition of attackers by information encryption, while attackers can learn which information belongs to secret information according to the encrypted information, so they can destroy the information even though they cannot decode the information, and receivers cannot read the secret information thereby.

2.2 Information hiding technology model

The three main links of information hiding technology are algorithm embedding, hidden information detection and hidden information extraction, and corresponding algorithms shall be used in hidden information detection and extraction. Algorithm embedding can be used in secret information hiding with secret key method, thus corresponding hidden carrier can be obtained after completing algorithm embedding. Hidden information detection and extraction can realize perception and recovery of the secret information in hidden carrier via the corresponding secret key, of which the secret key contains corresponding algorithm. When not possessing corresponding decoding secret key, attackers are hard to detect the secret information in hidden carrier and harder to steal and tamper the secret information. Generally speaking, secret information hiding and extraction pattern is as shown in figure 1.
2.3 Basic characteristics of information hiding

Basic characteristics of information hiding can mainly be divided into the following four aspects: First, the information possesses imperceptibility. Hidden carrier and original carrier are very approximate in characteristics, and the human cannot perceive change of the hidden carrier in vision and hearing and distinguish hidden image from original image with naked eye. Certainly, watermark visibility treatment can be given in some particular cases; Second, hidden carrier possesses robustness, which is mainly reflected in that hidden carrier still possesses the function of recovering secret information when suffering interference in certain degree, and the interferences suffered by hidden carrier mainly include distortion compression, smoothness, filtering, A/D transform, geometric transform, artificial destruction, enhancement, D/A transform and re-sampling, etc; Third, information hiding technology provides protection with secret key, so it possesses security. The secret information can be protected by secret key by applying information hiding technology, and it can obtain very strong attack resistance ability via algorithm embedding, thus secret information can be protected from being destroyed by attackers. Four, the information hiding technology shows great information hiding amount, and it needs to be noted that the greater hidden information amount may represent the worse robustness characteristic shown by hidden carrier.

3. RESEARCH ON THE DUAL DIGITAL WATERMARK ALGORITHM BASED ON INFORMATION HIDING TECHNOLOGY

3.1 Design thought and overall framework of the algorithm

When building dual digital watermark algorithm with information hiding technology, algorithm embedding and algorithm detection shall be contained (Gong et al.,2010). Thus, at least two inputs shall be possessed in algorithm embedding process, namely watermark information and carrier data, of which the watermark information embedding refers to the process of giving necessary algorithm treatment to such contents as image and character and then using them as the watermark signals for embedding in hidden carrier, and the carrier data refers to the relevant digital carrier works needing watermark embedding. Watermark embedding part is for output of the carrier work with watermark, so as to ensure transfer and transcription of the carrier work with watermark. When receiving the carrier work with watermark from channel, receiver can judge existence of watermark with the detection function. If the watermark exists, watermark signal can be extracted, and then it can be used in copyright detection and identification. When building dual digital watermark algorithm based on information hiding technology after analyzing the aforementioned functions, this paper shall give predetermination to the main functions in overall framework. After completing determination of main functions, simple treatment shall be given to the two watermarks needing embedding, and then the two watermarks after treatment shall be embedded in carrier. When carrier work needs to be given property right identification, the embedded digital watermark shall be detected and then be separated and extracted, and corresponding evaluation and test shall be given to correctness and quality of the two digital watermarks further.

3.2 Process of the dual digital watermark algorithm

A dual digital watermark algorithm is composed of three parts, namely watermark generation, watermark embedding and watermark detection and detection. According to the different application fields, emphases of the three parts are also different (Ma and Zhang,2003). Figure 2 is the watermark embedding flow chart.
In this figure, W represents watermark information, I represents original carrier data, and K represents the public key/private key for selection. There are various types of watermark information which can be in any form. G represents watermark generation algorithm, and W can be generated by virtue of random number generator. Thus, we can obtain the formula of watermark embedding process, namely \( I_w = (I, W, K)E \), in which \( I_w \) represents the data formed after watermark embedding, namely watermark carrier data, I represents the original carrier data, K represents combination of secret key, and W represents the original watermark information (Zhang, 2014). Watermark detection process flow chart is as shown in figure 3.

\[
W = (I_w, K, I)D \quad \text{when detecting no original watermark information existed in carrier,}
\]

\[
W = (I_w, K)D \quad \text{when detecting the original watermark information W existed in hidden carrier, and}
\]

\[
W = (I_w)D \quad \text{when detecting no original watermark information.}
\]

In these formulas, W represents estimated watermark, and \( I_w \) represents watermark carrier data. Watermark detection is mainly divided into the following two conditions: firstly, when there is no original watermark information, distribution hypothesis test or full search test shall be given to the embedded information; when there is original watermark information, correlation verification or extraction shall be given to the embedded signal. Watermark similarity test formula is \( Sim = \frac{WW}{\sqrt{WB} \sqrt{BB}} \), of which B represents the estimated watermark, W represents the original watermark, and Sim represents the similarity of signals.

### 3.3 Dual digital watermark algorithm analysis

In the dual digital watermark algorithm based on information hiding technology, the watermark embedding process refers to the process of giving pretreatment to watermark, generating corresponding watermark information and embedding the watermark information in the original carrier digital products (Xin, 2005). Watermark information is represented by \( C=\{c(i)\} \), and carrier digital product is represented by \( P=\{P_0(i)\} \). Thus, watermark embedding process algorithm can be presented by \( P_c = P_0(i) \cup h(i) \cup c(i) \) of which \( H=ht(i) \)
represents weighted handling and camouflage of watermark, and \( U \) represents overlay treatment. The most common two watermark embedding rules are additive embedding rule and multiplying embedding rule, and then rule formulas are \( P_c = P_0 + c(i) \times h(i) \) and \( P_c = P_0 \times (1 \times c(i) \times h(i)) \) respectively, of which \( P_0 \) represents time domain/space domain (Yang et al., 2011). Embedded watermark strength can be represented by watermark weighting, and the higher watermark strength represents the better robustness of the hidden carrier after information hiding, while it may have certain influence on watermark transparency, so we shall give consideration to the two aspects simultaneously to obtain better effect. However, during watermark detection process, the two detection methods of blind watermark detection and non-blind watermark detection shall be divided according to necessity of the original carrier digital product. When seeing from detection efficiency, it can be known that the higher detection efficiency represents the better reliability, so non-blind watermark detection is generally used in watermark detection. Comparing with the blind watermark detection method, non-blind watermark detection method possesses advantages of high efficiency and wide range, while it is very likely to give misinformation.

### 3.4 Detection of the dual digital watermark algorithm

In this paper, such methods as chaos sequence and scrambling algorithm are adopted in the pretreatment of digital watermark and carrier image in the dual digital watermark algorithm, of which chaos sequence is generated by utilizing mixed optical bi-stable model and Logistic mapping function, and scrambling algorithm is generated according to magic square scrambling and Arnold. In this research, multiple algorithms are used in digital watermark embedding, including HVS adaptive algorithm, LSB algorithm, DWT algorithm and DCT algorithm, and dual watermark embedding is realized by adopting these algorithms (Yang, 2011). When embedding digital watermark, it needs to find out the watermark area with the most obvious robustness, and to embed such relevant information as algorithm, digital watermark and sign on the basis of ensuring that carrier transparency cannot be impacted greatly (Yu et al., 2006). If information cannot be detected during information detection, the designated extraction algorithm can be used in the extraction of digital watermark in carrier, and corresponding extraction function can also be used in extraction, and workers shall judge whether the extraction should be successful.

### 4. CONCLUSIONS

To sum up, the dual digital watermark algorithm built by combining information hiding technology with digital watermark technology can realize efficient completion of the system in the links of watermark pretreatment work, watermark embedding, watermark detection, watermark extraction and various functions execution, and the application of VS.NET in system development can realize comprehensive application of dual watermark algorithm and such multiple digital watermark algorithms as DWT algorithm and LSB algorithm. By applying the dual digital watermark algorithm, the system can give consideration to robustness of watermark algorithm and transparency of digital watermark simultaneously, and it can possess very strong attack resistance performance, thus the system can give detection and index evaluation to copyright of the carrier work in various attacks, and information security and stability can be promoted greatly thereby.

### ACKNOWLEDGMENTS

Fund Program: Research and practice of higher education reform in Hebei(031041411); Key projects of teaching reform in LangFang Teachers University(K2015-10); Science and technology project of Hebei Province(15210707); Key scientific research project of LangFang Teachers University(LSLZ201502).

### REFERENCES


