Asia-pacific Journal of Convergent Research Interchange
Vol.9, No.4, April 30 (2023), pp.1-15
http://dx.doi.org/10.47116/apjcri.2023.04.01

A Research on Information Security Based on Digital Watermarking

Hye Jin Kim[1], Nam-Kyun Baik[2]

[1] *Ph.D. Course Student, Dept. of Smart Convergence Security, Busan University of Foreign Studies, South Korea, 20225432@office.bufs.ac.kr*

[2] *Professor, Dept. of Cyber Security, College of Science and Technology, Duksung Women's University, South Korea, namkyun@duksung.ac.kr*

Corresponding Author: Nam-Kyun Baik

Abstract: Researchers in the fields of information security and computer image processing are deeply concerned about digital watermarking technology as piracy of digital products like images, audio, video, and files, which are becoming increasingly serious due to the Internet's rapid development and the media resources' digitalization. By detecting the watermark information embedded in the digital media to identify the media copyright, the copyright of the digital media can be effectively protected. In fact, digital watermarking has important application value in covert communication, bill anti-counterfeiting, digital signature, fingerprint identification, logo implicit authentication, and so on. In this paper, an algorithm- and algorithm-combination-based dual digital watermarking design technique is proposed. Based on a careful examination of the algorithms and algorithms one at a time, this creative proposal combines the two algorithms to achieve efficient embedding and extraction of digital watermarks and to take advantage of the double watermark's security benefits to encrypt the transmission of digital maps, thereby enhancing the security of image transmission. Then, the scheme is tested to prove its feasibility. At the same time, in order to verify the advantages of the scheme, a variety of attack experiments are carried out on the scheme, and the experimental data in the same environment are compared with other dual digital watermarking schemes. Finally, the superiority and robustness of the scheme are obtained, and it is applied and popularized in the military. The emphasis of this paper is to realize the information security of armored mechanized troops. During the battle, armored mechanized units use the positioning system equipped by armored vehicles to snap the geographical environment of the battlefield instantly, and upload the image to the rear combat command center in time through the network, military network, and people's network. In this long-distance transmission process, in order to ensure the security and timeliness of the transmitted images, it is necessary to use encryption technology to protect and verify the military images.

Keywords: Double Digital Watermarking, Information Security, SVD, Industrial Security

1. Introduction

1.1 Research Background and Significance

With the rapid development of computer networks and communication technology, digital multimedia, including digital image, digital video, and digital audio, has been widely used. However, the security of digital media as well as the protection and authentication of intellectual property rights

Received: December 06, 2022; 1st Review Result: January 20, 2023; 2nd Review Result: February 19, 2023
Accepted: March 31, 2023

have become increasingly prominent. It is embodied in the following aspects: low replication cost. Different from traditional media, digital products have two characteristics: easy copying and low cost. As long as an individual publish a computer painting that he or she has worked hard to create online, a large number of copies will appear in a very short time. Even if you need to copy it in large quantities, it's just a matter of lifting a finger. Second, the quality of the copy has no loss and cannot be confirmed. When it comes to digital products, a lot of copies may be made quickly and with little quality loss when compared to the original versions because of computers' large-scale copying capabilities. Theoretically, even if a digital work is reproduced and copied indefinitely, the quality of the digital work will not be reduced. It is also difficult to distinguish who is the creator of the work and who is the reproducer of the work for a large number of quality-lossless pirated products. This is also the root of the rampant piracy of digital works and the difficulty in tracing infringement. Under the conditions of previous analog technology, the quality of any reproduction, whether film, audio tape, or video tape, would be lower than that of the original product, which made the cost of large-scale reproduction and dissemination very expensive, thus limiting the development and spread of piracy. The emergence of digital products has broken through the bottleneck problem of traditional media reproduction quality decline. Although the existing information security protocols can guarantee the security of digital products in transmission to a certain extent, with the increasing mainstream of digital products, the previous connection-oriented security technologies will be pale and powerless in the face of these new information security problems. At present, many countries have formed a set of standard solutions for the authenticity identification of artworks and paper documents, such as handwriting identification and paper identification. If these schemes are applied to the identification of digital products, they will be powerless. First, the duplicate digital products are 100% identical to the originals, which makes it impossible to distinguish them theoretically. Second, even while the document itself contains some extra information—such as the owner's name, the time it was modified, an identity password, etc.—because of how readily it can tamper, it only has a limited impact on identifying the person. Third, the creators of digital products lack sufficient proof of their identity because it is impossible to determine the authenticity of digital products. Therefore, digital product infringement forensics has become a difficult problem in the process of intellectual property law enforcement. With the continuous development of computer and network technology, the rapid improvement of domestic informatization level, the gradual popularization of e-government and e-commerce, and the transformation of the original business through information technology, more and more government departments, enterprises, and institutions are gradually changing to "paperless" office work. With the development of the application technology of "document image", paper documents are quickly converted into "pictures" or "pictures and texts" databases, which provide users with quick inquiry and information release in combination with the working characteristics, and assist the existing information system to integrate all work links into the "Internet". In view of this, under the premise of making full use of various conveniences brought by the Internet, how to improve the information security protection ability of products, and implement effective copyright protection for digital products will become a real problem to be solved[1].

At present, the economic losses caused by piracy are very large. According to the report of the American Film Association, the film industry lost billions of dollars due to piracy; hence, our country lost billions of dollars. The ways of piracy mainly involve free downloading on the Internet, buying pirated copies, and buying genuine copies. The pirated contents are mainly music and movies, literary works, software, online games, etc. In the aspect of multimedia protection, if it is realized by encryption, that is, digital multimedia is encrypted into secret text and then released, and illegal attackers can't get the original data from the encrypted text during transmission, thus achieving the purpose of copyright protection. But this approach has not completely solved the problem. The fact that encrypted digital products are rendered invisible or inaudible limits the efficient circulation of digital information, and encryption makes it easier to draw the attention of unauthorized attackers, which increases the likelihood

of being cracked. At the same time, once the original data is decrypted, it will become transparent and completely lose the possibility of copyright protection[2]. Therefore, a new copyright protection technology is needed to protect the copyright and security of multimedia. Digital watermarking is an information security technology developed in recent years, which belongs to the category of steganography, a branch of cryptography. It makes use of the redundancy of multimedia data to embed information related to the copyright of works into multimedia works. Through hidden information in multimedia works, we can confirm the creator and buyer of multimedia products, or judge whether the content is true and complete, so as to achieve the purpose of copyright protection[3]. Watermarking technology has shown a good prospect as an effective means to solve the problem of copyright protection since it came into being, which has aroused the widespread concern among some research institutions and companies at home and abroad. Since the digital watermarking technology was officially put forward in the 1990s, some famous universities and research institutions in Europe and America, such as the United States, universities, Cambridge University in England, a university in Germany, research institutes, etc., have invested considerable manpower and financial resources and achieved certain results. Some companies have launched digital watermarking software products, such as Highwater FBI, Digimarc-Corporate Rion, and so on.

1.2 Related Works

More than ten years have passed since the invention of digital watermarking technology[1-3], and in that time, its quick advancement and widespread use have garnered the support and attention of several large corporations and academic communities both domestically and abroad. The institutions that support and carry out digital watermarking research abroad include well-known enterprises and universities, as well as military and government departments, such as companies, Philips of the Netherlands, Watson Research Center of IBM, CA, Cambridge Research Institute of Microsoft, Lucent Bell Laboratories, Research Institute, Massachusetts Institute of Technology, Cambridge University, University of Illinois, University of Minnesota, Federal Institute of Technology in Lausanne, Switzerland, Vigo University in Spain, US Air Force and Army Research Institute, US Treasury, and German National Information. Due to the high attention of these companies or institutions and the strong support of human and financial resources, many achievements have been made in digital watermarking. Among them, the American company first introduced its own watermarking technology, and enjoyed the patent right of this technology, so it became the only company with this technology in the world at that time. Since then, this technology has been widely used in Photoshop4.0 and CoreDraw7.0, but it also has a disadvantage in that it is not robust enough to embed and extract the detected watermark. For this reason, the company launched a new watermark reading software in October, which can be used to find out whether the image contains a watermark and its information content, but the effect is still not satisfactory. In 2000, the first report on image data hiding appeared in the US government report. In addition, Japan, Britain, and other countries also started in-depth research on this technology in the early 1990s, which has played a certain role in promoting the development of digital watermarking technology. With the deepening of the research on digital watermarking technology, relevant international conferences, and related documents have been held and emerged. The first paper on digital watermarking was born in, and since then, the number of literature on this aspect has been increasing day by day. Some important and authoritative international journals, such as Proceedings of IEEE, IEEE Transaction, Signal Processing, IEEE Journal of Selected Area on Communication, Communication of ACM, etc., have successively published special issues of digital watermarking. As well as some influential international conferences such as IEEE ICIP, IEEE ICASSP, SPIE, ACM Multimedia, etc., not only published albums, but also opened up relevant thematic discussions. For example, with the efforts of foreign scholars and technical experts in watermarking, the first international symposium on

information hiding was held. So far, it has been successfully held ten times. The first four sessions were held in Cambridge, England, Portland, Germany, and Pittsburgh, USA. The 10th session was held in California, USA. Not only that, foreign research scholars also actively carry out academic exchanges and cooperation. For example, the International Conference on Image Processing was successfully held in, and two thematic discussions on new digital watermarking technologies and algorithms were specially opened at the conference. Since this year, the International Society of Optical Engineering has held a regular conference on multimedia information security and digital watermarking every year, the contents of which are mostly the latest research results and important research papers on digital watermarking technology. The success of these conferences not only promoted the rapid development of digital watermarking technology, but also increased the communication between researchers. Up to now, there are much foreign literature on digital watermarking research, and thousands of literatures and papers have been published one after another. Many websites have also opened digital watermarking research forums for everyone to exchange and discuss. All these efforts will definitely promote the research, development, and application of digital watermarking technology. In practical application, digital watermarking technology embeds the watermark signal into the original digital information to obtain the final version of digital products for distribution. When a copyright dispute occurs, extracting or detecting the watermark by a third party can effectively protect the legitimate rights and interests of copyright owners and legitimate users on the one hand, and crack down on illegal behaviors of illegal users on the other.

2. Introduction of Digital Watermarking

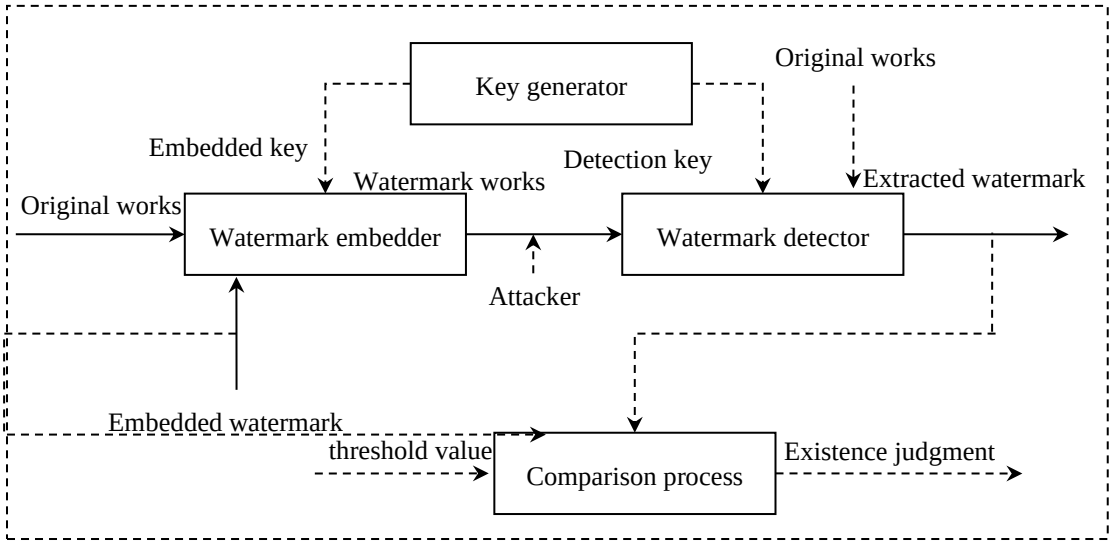
2.1 Overview of Digital Watermarking

Papermaking, one of the four great inventions, was invented more than a thousand years ago in China, but in fact, the paper watermark was not born in Italy until. That is, before this year, people invented the watermark on paper in hand-made paper technology. The thin line templates that are added to the paper mold during the manufacturing process give the area where thin lines are present a thin, usable appearance, giving the watermark of this invention a transparent appearance. The initial use of watermarks is reflected in the paper market. In the origin of the invention of the watermark in a town in Italy, the invented watermark is widely used in the paper industry by the people of the town. At the end of that time, there were about 10 paper mills in the town, all of which used the paper market and produced a paper with different specifications. At that time, the raw paper produced by the paper mill had a rough surface and could not be used directly. Therefore, this raw paper material needs to be handed over to other craftsmen for secondary processing. These craftsmen use a kind of hard stone called a polishing machine to smooth the surface of the paper, and then check it out, and finally resell it to merchants. These merchants first store them in the warehouse, and then put them on the market for sale when the price is high or capital turnover is needed, from which they can get high-profit returns. In view of this, the consequence of high profits is that not only the business competition between home paper mills is fierce, but also the industry competition among craftsmen and businessmen is fierce. For any party, in order to ensure the quality of the paper industry, it is not a simple and easy task to track and identify the sources and specifications of paper in time. In this case, using a watermark is a good solution, which can eliminate the possible conflicts between peers. Therefore, at that time, watermark, as an effective means to ensure the specification and quality of paper, will mainly be the task of identifying the factories that produce paper. The term "watermark" really came into being at the end of the century, and it originated from German vocabulary. Since water plays a relatively minor role in the paper-making process and the watermark's integration into the paper industry, the word "watermark" is actually misleading. Perhaps it is because the watermark has an effect similar to that of water on paper that this

word is formed. However, while the "watermark" technology comes into being, it also gives the counterfeiters an opportunity. It is sensitive to discover that this technology can be used to forge watermarks used in paper money anti-counterfeiting. We say this is illegal and undesirable, but it is the update of this forgery technology that promotes the development of watermarking technology invisibly. The earliest appearance of electronic watermarking technology originated in the United States in.

At that time, Muzac applied for a patent named "identification of picture and like signal". This patent solves the problem of embedding an artificially specified identification code into music in an invisible way. When there is a dispute, the copyright owner can be identified by extracting this identification code. Subsequently, with the vigorous promotion of many scientific researchers and some famous research institutes, digital watermarking entered a period of rapid development until the early 1990s. The representative one is the research and application of digital image watermarking, and many new algorithms have emerged. Besides, the research on audio and video watermarking has also developed to some extent, although the research on video watermarking started late, However, there are also new improvements, such as K.Matsui's research and the concept of video steganography, Frank Hartung's attempt to embed copyright information in original and compressed videos according to the spread spectrum principle, etc., and thus various video watermarking technologies have come out one after another. Due to the limitation of computational complexity and standard video coding and decoding system, although domestic and foreign researchers, experts, and scholars have conducted in-depth research on digital video watermarking technology and made some research results, compared with image watermarking, the research work in this area is still very weak. In view of the historical origin of the above-mentioned digital watermarking and the research situation of digital watermarking by Juqian, digital watermarking can be defined as follows: embedding marks or other information in the content of digital carrier, and the embedded marks or other information are generally imperceptible. After reading and calculating by some programs, the embedded marks or other information can be extracted or detected. In the process of embedding the digital watermark into the carrier information, it develops rapidly because it can bear some operations that do not damage the use value or commercial value of the source carrier data, such as proving the authenticity of products, protecting media copyright, tracking piracy or providing additional information of products.

2.2 The Framework of Digital Watermarking



[Fig.1] General Framework of Digital Watermarking

The general framework of digital watermarking is shown in [Fig. 1]. Among them, the solid line indicates the necessary steps in the process of watermark embedding and detection, and the dotted line indicates the possible steps. The main steps are as follows: firstly, the original work O, the digital watermark W and the key K(K1,K2) are used as the input keys, which are mainly used for encoding, specifying the embedding position or encrypting the watermark information, embedding the watermark information into the carrier work through a certain watermark algorithm embedder to obtain the watermarked work containing the watermark, and then extracting the watermark information through a watermark detection algorithm watermark detector. At this time, according to whether the original works are needed to extract the watermark, we divide the detection algorithm into blind detection which does not need the original works, and detection which contains auxiliary information which needs the original works. Finally, according to the similarity between the extracted information and the original watermark, we can determine whether the carrier works contain the watermark or not by setting a certain net value.

2.3 Characteristics of Digital Watermarking

(1) Imperceptibility

For digital watermarking, this is the most basic characteristic. For people's visual system, the change of the original information caused by the embedding of digital watermarks should be subtle and imperceptible, and it will not interfere with the normal legal transmission of the original data in any case. Furthermore, for a large number of digital information embedded with the same digital watermark by using the same watermarking algorithm, it is impossible to extract the watermark or determine the existence and location of the watermark even by using the probability statistics method.

(2) Robustness

Robustness is very important for digital watermarking. Robustness refers to the robustness of the digital watermark, that is, the digital watermark must be difficult to remove from the embedded digital information, and difficult to be destroyed and forged. Specifically, digital watermarking should be able to resist general signal processing noise, smoothing, filtering, centering and conversion, compression, etc. and various geometric transformations such as translation, rotation, scaling, clipping, etc. After these processes, the robust watermarking algorithm should still be able to extract the embedded watermark or prove its existence. If an attacker tries to delete the watermark, the original data will be completely destroyed. If you don't have all the relevant knowledge of the watermark, the digital watermark can hardly be forged.

(3) certainty

The information carried by digital watermark can be uniquely identified, providing complete and reliable evidence for the ownership of information products protected by copyright, and at the same time monitoring the spread of protected data to prevent illegal copying. In fact, this is the driving force behind the development of watermarking technology.

(4) universality

A good watermarking algorithm should be widely embedded in different original information at the same time, such as text, image, audio, and video, so as to solve the digital watermarking problem of multimedia products. Digital watermarking should have considerable data capacity to meet the demand to diversified texts, signs, serial numbers, and so on.

Among these characteristics, imperceptibility, robustness, and data capacity conflict with each other, this restricts the concrete implementation of the watermarking algorithm[4-6]. In order to obtain better robustness, the embedded watermark strength should be as high as possible, which affects the imperceptibility of the watermark. In order to obtain a larger data capacity, the embedded watermark information should be as much as possible, which will also be difficult to guarantee the imperceptibility

of the watermark[7][8]. At this point, a good compromise is needed.

2.4 Classification of Digital Watermarks

In practice, we can classify watermarks simply.

(1) Private watermark and public watermark

The scheme that the original data must be used in watermark detection is called private watermark, and the scheme that does not need the original data is called a public watermark. When the copyright owner identifies the illegal copy according to the private watermark, it must be taken as evidence together with the original information product.

(2) Symmetric watermarking and asymmetric watermarking

Symmetric watermarking means that the embedding of the watermark is the same as the detection key. Like cryptography, the security of digital watermarking can't be guaranteed by a secret algorithm. Under the condition that the watermark algorithm is public, if the attacker knows the key, he can easily delete the watermark, so the watermark key is generally not public at present. In order to make watermarking more convenient and safer, the concept of asymmetric watermarking is proposed. Asymmetric watermarking requires the public detection algorithm and key, so that anyone can easily detect the watermark, but can't delete the embedded watermark 1 according to the detection algorithm and key.

(3) Robust watermarking and fragile watermarking

Digital watermarking can also be divided into robust watermarking and fragile watermarking .A robust watermark refers to a watermark that can't be modified or removed under a malicious attack. A fragile watermark means that any processing of a work will destroy the watermark. A fragile watermark is generally used for content authentication, and whether the content has been modified or not can be judged by detecting the watermark. The least significant bit of watermark in the time domain is a typical fragile watermark. If the watermark can withstand reasonable distortion, but it will be damaged by unreasonable distortion, it is called a semi-fragile watermark.

(4) A perceptible watermark and an imperceptible watermark

This classification is mainly based on whether it is visible or not. The most common example of perceptible watermark is the translucent logo on cable TV channels or images, whose main purpose is to clearly identify copyright and prevent illegal use. The imperceptible watermark is completely hidden, so that when piracy occurs, the watermark can be extracted as evidence to punish the pirates.

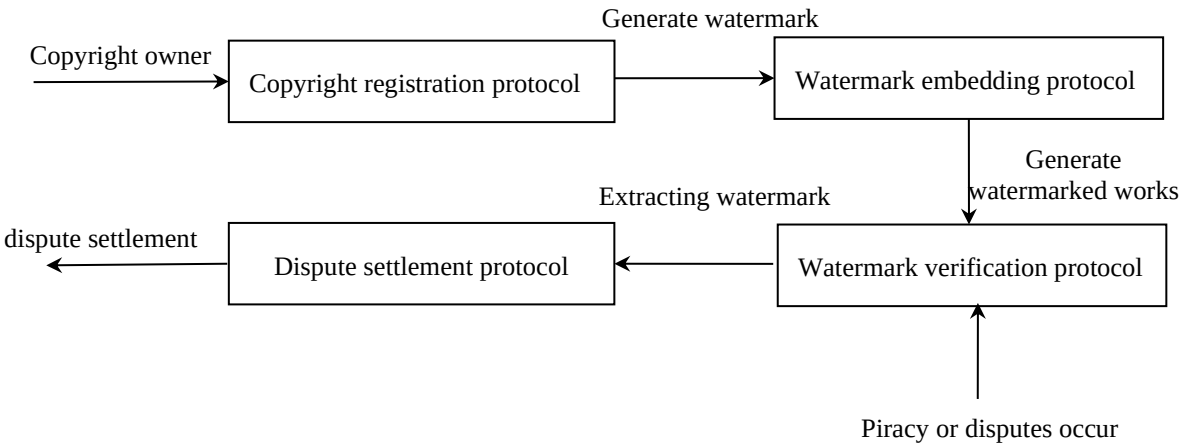
(5) Time-space domain watermarking and transform domain watermarking

Temporal-spatial digital watermarking technology is to hide the watermark by modifying the signal samples in temporal-spatial domain. The least significant bit of watermark is a common time-space watermark. Transform domain watermarking technology hides the watermark by modifying transform domain coefficients. Commonly used transform domain methods include discrete Fourier transform, discrete cosine transform, discrete wavelet transform, and so on[9].

2.5 Digital Watermarking Protocol

Watermarking protocol refers to a series of steps taken by participants to protect the copyright of multimedia digital products by using digital watermarking and other technologies[10]. For example, whether the copyright owner generates the watermark or the authority generates the watermark, whether the copyright owner embeds the watermark or the third party embeds the watermark, and whether the third party needs to participate in the dispute. Others put forward the prototype of the digital watermarking protocol, which laid the foundation for future research of digital watermarking protocol. In 2000, a formal digital watermarking proposal between buyers and sellers was put forward. An

anonymous fingerprint protocol is proposed. With the development of digital watermarking technology, the watermarking protocol has been continuously improved. The general framework of the watermark protocol is shown in [Fig. 2], which generally includes copyright registration protocol, watermark embedding protocol, watermark verification protocol, and dispute arbitration protocol.



[Fig.2] General Framework of Watermarking Protocol

(1) Copyright agreement

The copyright registration agreement mainly involves the registration of copyright and the generation of watermarks. Whether the watermark is generated by the copyright owner or by a third party mainly involves the credibility of the watermark. In general, establishing a secure channel with the authority, registering the copyright of digital works with the authority, and obtaining the digital watermark notarized by the authority is a good solution for the secure watermarking protocol.

(2) Watermark embedding protocol

Watermark embedding protocol mainly involves how and who will embed the watermark. Generally, watermark embedding can be done by a watermark embedding program jointly run by the buyer and the seller or by a watermark embedding server of an authority. Considering that if the watermark embedding server of the authority is used to embed the watermark, it may involve the transmission of a large number of digital works with the authority, which will bring a lot of inconveniences, so the copyright owner usually completes the watermark embedding work. Watermark embedding protocol should not only ensure the security of communication channel, but also ensure the validity of watermark for digital works and the confidentiality of watermark data.

(3) Watermark verification protocol

When the copyright of a digital work is violated, the digital watermark of the work can be verified by the watermark verification protocol to determine the possible copyright owner of the digital work. In the process of watermark detection, we must consider the security of the watermark and watermark key. For the traditional symmetric watermarking scheme, the watermark embedding key and the detection key are the same. Therefore, in the process of watermark detection, the watermark embedder needs to provide the detection key. However, this will bring inconvenience to the detection process, which can only be carried out with the participation of the embedder. Once the detection key is leaked, it will threaten the security of the watermark, and make criminals use the detection key to embed or remove the watermark. Generally, there are two ways to solve the above problems, one is to use the traditional public key cryptosystem, with the private key as the embedded key and the public key as the detection key, and the other is to use the zero-knowledge proof method. The zero-knowledge watermark verification scheme makes use of the idea and algorithm of zero-knowledge proof in cryptography,

which can convince the watermark verifier that the watermark exists without revealing the watermark key. He Yongzhong et al. proposed a publicly verifiable zero-knowledge watermark detection protocol, which can prevent fuzzy attacks and be publicly verifiable, and reduce the dependence on third parties.

(4) Dispute arbitration agreement

When the copyright owner of digital works can't be solved by digital watermarking technology alone, such as different watermark data detected in the works or the watermark data can't be recovered due to too much damage to the works themselves, both parties need to arbitrate according to the arbitration agreement. The arbitration is based on the data specified in the arbitration agreement and is closely related to the above agreements. In the actual design of the watermarking protocol, most of them need to make use of the existing perfect cryptographic system and some mature watermarking embedding and detection algorithms, such as encryption and decryption, digital signature, digital certificate, etc., while the watermarking algorithm requires high robustness.

3. Double Digital Watermarking Scheme Based on SVD and DFT

With the wide use of digital watermarking in digital products, human beings are increasingly aware of its importance, thus prompting many experts and scholars to conduct in-depth research on digital watermarking, which has made a qualitative leap in the development level of digital watermarking, that is, from the original one-watermark design scheme to the present two-watermark design scheme or even multiple-watermark design scheme. With some experts and scholars' deepening research on the application of dual digital watermarking in image processing, some digital watermarking papers have been published one after another in the research of combining the two, but so far, there is no such research paper published in the research of dual digital watermarking combined with the two. Therefore, this paper puts forward a dual digital watermarking scheme that combines the two. On the basis of embedding the watermarked image, the watermarked image is verified and embedded, so as to embed the host image with dual watermarking. Finally, the feasibility of this dual watermarking scheme is proved by theoretical and experimental results.

3.1 Research on SVD and DFT Algorithms

3.1.1 Research Status of SVD Algorithm

With the continuous research of digital watermarking algorithms, the watermarking algorithm of singular value decomposition has attracted people's special attention. Liu proposed a digital watermarking algorithm based on in 2002 for the first time. In this algorithm, the watermark matrix is superimposed on the singular value matrix, and the left and right singular matrices in singular value decomposition need to be provided in the process of watermark extraction. "A hundred flowers blossom, a hundred schools of thought contend", in the following period, many researchers published some literature books successively, and put forward some similar algorithms according to this method, among which the singular value decomposition watermarking algorithm based on quantization was put forward in, which divided the image into blocks, then decomposed the singular value, quantified the largest singular value and then embedded the watermark, thus solving the blind extraction in the watermark extraction process. These two kinds of methods basically represent the current digital watermarking technology based on SVD[11-13]. The attacks that digital watermarking technology often faces are digital signal processing and geometric distortion of geometric processing operations. Usually, digital signal processing attack refers to the conventional processing of the signal containing watermark information, such as conversion, knife conversion, filtering, noise addition, resampling, image enhancement, lossy compression, etc. Generally speaking, this kind of attack is not necessarily malicious, but it is likely to destroy the watermark. Geometric processing operation, also known as

geometric distortion intestinal attack, refers to the sequence of operations such as rotating, cutting, scaling, deleting, inserting sampling points, and even printing, reprinting, and scanning signals. In fact, this kind of attack did not destroy the watermark, but only destroyed the synchronization of the detection software in the detection process, so it could not extract the watermark correctly or find the exact location of the watermark because of its distortion. Usually, the solution to this kind of attack is to consider the damage to private watermark and public watermarks, estimate the geometric distortion by feature matching or template embedding, and then extract or detect the watermark, but the effect of this method is not very ideal. Experiments show that it has good theoretical support for resisting geometric distortion attacks. The application of SVD theory in digital image processing is embodied in linear algebra. A digital image can be regarded as a matrix composed of many non-negative scalars.

3.1.2 Research Status of DFT Algorithm

Discrete Fourier (DFT)[14] Transform association is widely used in digital image processing because it establishes the relationship between discrete time domain and discrete frequency domain in digital signal processing. In the process of digital signal processing, if convolution and correlation operations are directly used for processing in the time domain, the calculation amount of the computer will increase, and the calculation amount will increase with the square of sampling points, which will not only take time, but also be difficult to meet the requirements of real-time processing. In general, the signal is transformed first, and then processed in the frequency domain. This has the advantage of reducing the amount of calculation, making the processing more convenient, and the processing speed is also improved compared with that in the time domain. At present, with the in-depth study of discrete Fourier transform, some literature has been published. In this algorithm, the length from the center to the vertex of the model is calculated first, and then it is transformed. Secondly, when embedding the watermark, it is realized by modifying the modulus of the coefficient. Finally, the global feature is taken as the embedding object, and a bit of watermark information is distributed in the whole model. However, compared with many current pieces of researches on digital watermarking algorithms, there are few pieces of researches on digital watermarking algorithms, and there is still great development potential. In practical application, it has important physical significance. From the physical point of view, Fourier transform is to transform the image from the spatial domain to the frequency domain, that is, to transform the gray distribution function of the image into the frequency distribution function of the image, and its inverse transform is to transform the frequency distribution function of the image into the gray distribution function. From a mathematical point of view, Fourier transform transforms a function into a series of periodic functions. Assuming that it is an analog signal with limited energy, its Fourier transform represents the spectrum. In general, the Fourier transform that directly handles discrete-time signals is known as the discrete Fourier transform. If a continuous signal is to be analyzed by a computer, it must be discretized because computers can only compute the sum of numbers. Therefore, the Fourier transform of the continuous signals integration process will change into the process of seeking sum.

Discrete-time signal refers to a signal that only takes values at a specific set of moments, but does not take values or has values at other moments. Digital signal refers to the signal which quantifies the amplitude of discrete signal discretely, and quantifies it into binary code sequence, that is, the signal represented by digital sequence. Generally speaking, images are two-dimensional, so we can use a two-dimensional matrix $z = f(x, y)$ to represent points in space. For example, images can be used to represent. As the two-dimensional discrete Fourier transform has many properties, such as translation, separability, rotation invariance, conjugate symmetry and periodicity, distribution and proportionality, average value, convolution theorem, correlation theorem, etc., this paper only introduces some of its main properties. Separability. Two-dimensional Fourier transform can be decomposed into one-dimensional transform in two directions. In other words, any two-dimensional Fourier transform or

inverse transform can be realized in two steps, and each step is a one-dimensional Fourier transform or inverse transform.

3.2 Double Watermarking Scheme Based on SVD and DFT

Double watermark, as its name implies, is to have two watermarks. In fact, it can be understood that there must be at least two watermarks, which also contains the implication of more than two watermarks, because some algorithms are probably embedded with watermarks. Obviously, the two watermarking algorithms are loaded together, but it is not said that double watermarking is only a new algorithm; one is a double watermark, and so on. At present, in view of the gaps in the literature on digital double watermarking combining with, this design is proposed, which is also the core content of this paper. Generally speaking, the watermark system is always composed of two parts: watermark embedding and watermark extraction, except for those that require special verification. Therefore, the overall arrangement of this paper is based on this idea, but the content is enriched and modified. The specific scheme is as follows.

Watermark embedding

Considering that the algorithm has strong robustness in the geometric distortion of the image and good anti-shearing ability, we choose these two algorithms for watermark embedding. In the overall design of the watermark embedding method, two frameworks are adopted, that is, firstly, the algorithm is used to embed the watermark to obtain the initial carrier image, and then the algorithm is used to embed the watermark twice on the obtained carrier image to obtain the carrier image with double watermarks, which is the second one. Before embedding the watermark into the carrier image, it is defined here.

For N*N matrix A, if there are n scalars $\lambda_i(i=1,2,\cdots,N)$ satisfying formula (1).

$$\left|A-\lambda_i I\right|=0 \tag{1}$$

This group can be called the unique eigenvalues of the matrix.

If there is such a vector of N*1, there is formula(2).

$$AV_i=\lambda_i V_i \tag{2}$$

Here, V_i is called a characteristic vector corresponding to the characteristic value λ_i. A has a total of eigenvectors.

Singular value decomposition (SVD) is the inherent characteristic of the matrix and plays an important role in digital image processing. Assuming moments here $A\in R^{m\times n}, rank(A)=r, r\le n$, then the singular value decomposition of matrix A is defined as formula(3).

$$A=UDV^T=\left[u_1,u_2,\cdots,u_m\right]\begin{bmatrix}\sigma_1 & 0 & \cdots & 0\\ \vdots & & & \\ 0 & 0 & & \sigma_r\end{bmatrix}_{m\times n}\left[v_1,v_2,\cdots,v_n\right]^T=\sum_{j=1}^{r}\sigma_j u_j v_j \tag{3}$$

Wherein, $U=\left[u_1,u_2,\cdots,u_m\right]\in R^{m\times m}$ and $V=\left[v_1,v_2,\cdots,v_m\right]\in R^{m\times n}$ is an orthogonal matrix, and its column vectors are u_i and v_i respectively; From here, U and V are the left and right singular matrices of the matrix respectively; D is diagonal matrix; $\sigma_i(i=1,\cdots,r)$ called the singular value of

matrix A. Here the positive square root of the eigenvalue of AA^T or A^TA, satisfies $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r > \sigma_{r+1} = \cdots = \sigma_m = 0$. Because the singular value λ_i of the matrix has good stability, that is, the moment when the array has tiny vibration, the change of its singular value will not be greater than the vibration matrix. Matrix decomposition can be used for image compression to some extent.

4. Experimental Results and Analysis of Double Watermarking Scheme

Up to now, with the efforts of some experts and researchers, some dual digital watermarking techniques and schemes have been developed one after another, such as the aforementioned robust digital watermarking algorithm[15][16] based on sum, digital image watermarking algorithm based on wavelet transform and singular value decomposition, color image dual watermarking algorithm based on wavelet transform and so on. It can be said that each of the above algorithms has its own expertise, which mainly depends on the user's research object and specific requirements. In view of this, at the beginning of writing, this paper also carried out a variety of experiments on the dual digital watermarking scheme studied. The experiments show that the scheme proposed in this paper has certain research value. This study compares this scheme with the dual digital watermarking scheme based on and uses an identical environment for the experiment in order to demonstrate its superiority. The selected carrier image, watermark size, experimental steps, and attack methods are all the same. The specific experimental data are compared and analyzed as follows.

(1) Comparison of noise experimental data

[Table 1] Experimental Data of Noise in SVD-DFT Attack Experiment

Add noise intensity		0.01	0.02	0.03	0.04	0.05
Salt and pepper noise	PSNR	21.453	18.546	16.601	15.550	14.599
(SVD)	NC	0.999	0.999	0.999	0.999	0.999
Gaussian noise	PSNR	13.990	13.986	14.016	14.021	13.991
(SVD)	NC	0.999	0.999	0.999	0.999	0.999

[Table 2] Experimental Data of Noise in SVD-DCT Attack Experiment

Add noise intensity		0.01	0.02	0.03	0.04	0.05
Salt and pepper noise	PSNR	18.903	15.951	14.294	12.922	12.011
(SVD)	NC	0.999	0.999	0.999	0.999	0.999
gaussian noise	PSNR	14.332	11.524	9.883	8.785	7.973
(SVD)	NC	0.999	0.999	0.999	0.999	0.999

The experiments all adopt the same image size and double watermark transformation. Through the above two groups of experimental data, we can see that the PSNR and NC values obtained in the SVD-DFT attack experiment, whether it is salt and pepper noise or Gaussian noise, are larger than those obtained in the SVD-DCT attack experiment, and the PSNR value is higher by 2-4dB on average, but the difference is only 0.0001-0. However, it is enough to prove that the scheme proposed in this paper can enhance the value of the sum of the image after the noise attack, improve the confidentiality of the image and minimize the visual difference, thus proving the security and robustness of the watermarking scheme.

Comparison of shear experimental data.

[Table 3] Cutting Experimental Data in SVD-DFT Attack Experiment

Add noise intensity		0.1	0.2	0.3	0.4	0.5
Salt and pepper noise	PSNR	14.835	9.125	6.860	6.053	3.793
(SVD)	NC	0.999	0.998	0.997	0.997	0.997
gaussian noise	PSNR	14.831	9.125	6.860	6.053	3.793
(SVD)	NC	0.938	0.919	0.918	0.917	0.884

[Table 4] Cutting Experimental Data in SVD-DCT Attack Experiment

Add noise intensity		0.1	0.2	0.3	0.4	0.5
Salt and pepper noise	PSNR	11.031	6.141	3.085	1.840	0.869
(SVD)	NC	0.999	0.999	0.997	0.997	0.996
gaussian noise	PSNR	11.031	6.141	3.085	1.840	0.869
(SVD)	NC	0.969	0.921	0.845	0.785	0.715

By comparing the data of [Table 3] and [Table 4], it is found that in these two dual digital watermarking schemes, the value of is far greater than the value of, which is higher on average. But at the same time, we also find that the scheme is not invulnerable, and the value obtained when the image is cut in these two tables is smaller than the corresponding value in the scheme. However, what makes us feel gratified is that the values obtained during image cutting, and cropping in the scheme are larger than the corresponding values in the scheme, and their values are all above this threshold, while the corresponding values during image cutting and cropping in the scheme are already smaller than this threshold, which is obviously a flaw. Comparison of rotating experimental data

[Table 5] Experimental Data of Carrier Image Rotation in SVD-DFT Experiment

Angle of rotation of image	90	180	270
PSNR	26.161	25.852	26.160
NC	0.999	0.999	0.999

[Table 6] Experimental Data of Carrier Image Rotation in SVD-DCT Experiment

Angle of rotation of image	90	180	270
PSNR	23.686	23.194	23.689
NC	0.999	0.999	0.999

The value of SVD-DFT dual watermarking scheme through [Table 5] and [Table 6] is much higher than that of SVD-DFT dual watermarking scheme, with an average of 2.4dB higher. Although the value of the SVD-DFT dual watermarking scheme is 0.0003-0.0004 lower than the NC value of the dual watermarking scheme, it has little effect on the identification of watermarks, and the values of dual watermarking schemes are far above this threshold. Considering the reliability of watermark extraction. To sum up, we can draw the following conclusion: For the dual digital watermarking scheme combining algorithm and algorithm, the above design and experiment prove the feasibility and robustness of this scheme. In the experiment, researchers set the threshold of the normalized correlation coefficient too. Through the experimental data, we can see that all the values obtained are larger than this closed value, which meets the needs of practical application, which is exactly what we expect.

5. Conclusions

This paper mainly discusses the application of digital watermarking technology in information security. On the content arrangement, firstly, some basic knowledge of digital watermarking is introduced, including the concept, framework, characteristics, and classification of digital watermarking. Then, the digital watermarking protocol is tracked dynamically, and the watermarking

preprocessing technology is summarized. Based on the detailed description of traditional image scrambling algorithms, a new image scrambling transformation algorithm, namely the diagonal equal replacement algorithm, is proposed through repeated experiments and verification. That is to say, on the basis of the traditional image scrambling transformation algorithm, by resetting the value of the mapping yin to make its diagonal values equal, and then changing the pixel points of the image by replacement, the feasibility, and robustness of the algorithm are proved by the experiment of restoring the image. Although digital watermarking technology has made rapid development in recent years, especially in still images, it has gained a lot, but the research and development of dual digital watermarking are still slightly insufficient, especially since the literature on this aspect is relatively few. With the wide application of information technology in the modern high-tech battlefield environment and the advent of the digital era, the military urgently needs dual digital watermarking encryption technology. Therefore, this paper proposes a design scheme of double digital watermarking based on algorithm and algorithm combination. On the basis of studying algorithms and algorithms one by one, this scheme creatively puts forward a design scheme that combines the two algorithms, realizes the effective embedding and extraction of digital watermarks, and makes use of the security advantages of double watermarks to encrypt the transmission of digital maps, thus improving the security of image transmission. After that, the simulation experiment of this scheme is carried out on the platform, which proves its feasibility. At the same time, in order to verify the advantages of this scheme, a variety of attack experiments are carried out on this scheme, and then the watermark is extracted. Besides, this scheme is compared with other double digital watermarking schemes in the same experiment. A large number of experimental results prove that this scheme has good superiority and robustness, and is feasible. This type of double digital watermark will, in part, serve the purpose of "confusing the audience" because, first, the other party cannot know the crucial information concealed in the common image; second, even in the event that the other party is aware of the information's concealment; and third, even if the opponent intercepts the carrier image, he may forget about it shortly after it has been extracted. With the rapid development of science and technology, it has a bright future and far-reaching significance to introduce dual digital watermarking technology into military affairs and apply it. Especially in this critical period of increasing digitalization and popularization of networking, the acquisition of information rights will ultimately determine which side the balance of victory will ultimately point to. Of course, it is not only military, but also civilian. Many scholars have also carried out in-depth research on this, but up to now, there are still little related literature in this field about the dual digital watermarking scheme proposed in this paper.

6. Acknowledgments

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ICAN(ICT Challenge and Advanced Network of HRD) program(IITP-2022-2020-0-01825) supervised by the IITP(Institute of Information & Communications Technology Planning & Evaluation) and This research was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea Government(MSIT) and Korea Institute for Advancement of Technology(KIAT) grant funded by the Korea Government(MOTIE) (P0008703, The Competency Development Program for Industry Specialist).

Reference

[1] P. Kadian, S. M. Arora, N. Arora, Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey, Wireless Personal Communications, (2021), Vol.118, pp.3225-3249.

DOI: https://doi.org/10.1007/s11277-021-08177-w

[2] S. Godhar, V. Kulshreshtha, Digital Watermarking Technique using DWT, SVD, and AES, SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, (2020), pp.116-121.

[3] V. Priyanka, S. Roop, A. Rajeev Ratan, Digital Watermarking Using DCT & DWT Technique, International Journal of Research, (2021), Vol.4, No.6, pp.1343-1348.

[4] B. Cheng, B. Zhang, Application of Robust Digital Watermarking Technology in Image Copyright Disputes, Journal of Physics Conference Series, (2021), Vol.1883.
DOI: https://doi.org/10.1088/1742-6596/1883/1/012124

[5] G. H. Yuan, Q. Hao, Digital Watermarking Secure Scheme for Remote Sensing Image Protection, China Communications, (2020), Vol.17, No.4, pp.88-98.
DOI: https://doi.org/10.23919/JCC.2020.04.009

[6] A. A. Embaby, M. Shalaby, K. M. Elsayed, Digital Watermarking Properties, Classification and Techniques, International Journal of Engineering and Advanced Technology, (2020), Vol.9, No.3, pp.2249-8958.

[7] U. Khadim, M. M. Iqbal, M. A. Azam, An Intelligent Three-Level Digital Watermarking Method for Document Protection, Mehran University Research Journal of Engineering and Technology, (2021), Vol.40, No.2, pp.323-334.
DOI: https://doi.org/10.22581/muet1982.2102.07

[8] J. G. Zhang, H. B. Qi, A Robust Digital Watermarking Algorithm Based on Finite-Set Discrete Radon Transform Tight Frame, Journal of Computer and Communications, (2020), Vol.8, No.12, pp.123-133.
DOI: https://doi.org/10.4236/jcc.2020.812012

[9] Q. F. Zhou, N. Ren, C. Q. Zhu, A. X. Zhu, Blind Digital Watermarking Algorithm against Projection Transformation for Vector Geographic Data, International Journal of Geo-Information, (2020), Vol.9, No.11, p.692.
DOI: https://doi.org/10.3390/ijgi9110692

[10] A. Meenpal, S. Majumdar, A. Balakrishnan, Digital Watermarking Technique Using Dual Tree Complex Wavelet Transform, 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), (2020), pp.62-67.
DOI: https://doi.org/10.1109/ICPC2T48082.2020.9071464

[11] V. Novakovi, S. Singer, A Kogbetliantz-Type Algorithm For The Hyperbolic SVD, Numerical Algorithms, (2022), Vol.90, pp.523-561.
DOI: https://doi.org/10.1007/s11075-021-01197-4

[12] T. S. Nguyen, Fragile Watermarking For Image Authentication Based on DWT-SVD-DCT techniques, Multimedia Tools and Applications, (2021), Vol.80, pp.25107-25119.
DOI: https://doi.org/10.1007/s11042-021-10879-z

[13] R. K. Singh, A New Image Watermarking Scheme Based on Block Conversion and DWT-SVD Approach, Internet of Things and Connected Technologies, (2021), Vol.1382, pp.262-277.
DOI: https://doi.org/10.1007/978-3-030-76736-5_25

[14] S. M. Xing, T. Y. Li, J. Liang, A Zero-Watermark Hybrid Algorithm for Remote Sensing Images Based on DCT and DFT, Journal of Physics: Conference Series, (2021), Vol.1952.
DOI: http://dx.doi.org/10.1088/1742-6596/1952/2/022049

[15] Z. Y. Liu, A. L. Wang, K. Xin, F. P. Liu, X. F. Zhu, Y. J. Ling, Z. C. Yu, Digital Holographic Watermarking Algorithm Based on DWT-DCT, Journal of Physics: Conference Series, (2020), Vol.1693.
DOI: http://dx.doi.org/10.1088/1742-6596/1693/1/012099

[16] U. A. Bhatti, L. W. Yuan, Z. Y. Yu, J. B. Li, S. A. Nawaz, A. Mehmood, K. Zhang, Multimedia Tools and Applications, (2021), Vol.80, pp.13367-13387.
DOI: https://doi.org/10.1007/s11042-020-10257-1

