International Journal of Innovative
Computing, Information and Control
Volume **17**, Number **4**, August **2021**

ICIC International ©2021 ISSN 1349-4198
pp. 1257–1274

MULTIPURPOSE MULTILEVEL MULTICHANNEL INFORMATION HIDING FRAMEWORK FOR MULTIMEDIA PROTECTION, AUTHENTICATION AND TRAITOR TRACING

Zhe-Ming Lu[1], Zong-Hui Wang[2,*] and Yong-Liang Liu[3]

[1]School of Aeronautics and Astronautics
[2]College of Computer Science and Engineering
Zhejiang University
No. 38, Zheda Road, Hangzhou 310027, P. R. China
zheminglu@zju.edu.cn; *Corresponding author: zhwang@zju.edu.cn

[3]Alibaba Group
No. 969, Wenyi West Road, Hangzhou 311121, P. R. China
yongliang.lyl@alibaba-inc.com

Received March 2021; revised May 2021

Abstract. *Nowadays, multimedia documents can be easily recreated or modified and then distributed over the Internet or via smart mobile phones; thus copyright protection, copy protection, content authentication and source tracing have become main issues in the big data era. In the past, many multipurpose information hiding schemes have been proposed to solve these problems. However, existing schemes are mainly designed for digital audiovisual documents, but seldom designed for office files, WEB pages, PDF files or software codes. Furthermore, there are few schemes considering how to embed multilevel fingerprints to trace multiple distribution processes. Based on above backgrounds, this paper presents a multipurpose framework based on multilevel multichannel information hiding to provide a more robust and conflict-prevented scheme with whole life cycle and full protection. This framework is developed for all kinds of multimedia documents to protect and/or authenticate and/or trace a multimedia document in its entire life time. In order to make our framework work better as an organic whole, we define a watermark information structure to discriminate and recognize different watermarks and also provide some required control information for watermark extraction or further embedding. To test the effectiveness of the proposed framework, we develop three simulation interfaces for images web pages and PPT files respectively. Experimental results demonstrate that our framework is effective and our scheme can embed multiple watermarks and can extract all watermarks correctly and independently.*

Keywords: Information hiding, Multimedia, Multipurpose multilevel multichannel information hiding, Copyright protection, Content authentication, Figerprinting, Traitor tracing, Annotation

1. **Introduction.** Nowadays, we have stepped into the era of big data due to the rise of computers, the Internet and technology capable of capturing information from the real, physical world we live in, and converting it to digital data. Multimedia documents can be easily generated, losslessly copied or deliberately modified and then transmitted over the Internet or via smart mobile phones to other users. Thus, copyright protection, copy protection, content authentication and source tracing have become four main issues in our era. The first generation of copyright protection and content authentication technology is cryptography [1,2] and digital signatures [3,4]. Cryptography can be used to encrypt multimedia documents to permit only valid keyholders access to encrypted data.

DOI: 10.24507/ijicic.17.04.1257

However, once the authorized person obtains the decrypted document, we cannot prevent him from reselling or revealing the decrypted document. In essence, a digital signature is the encrypted abstract of a document. During the transmission, the encrypted abstract can be used to demonstrate that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered during transmission (integrity). However, the digital signature should be attached in the document, which is easy to be removed by attackers. Furthermore, even a single bit is error, the document will fail to be authenticated, but for digital images, one bit error even more can be tolerated. Based on above backgrounds, information hiding [5,6] has been put forward since 1994 to serve as a new multimedia protection and authentication technique, which can be also combined with the traditional cryptography [7] and digital signature techniques [8]. The main advantage of information hiding is that the embedded information in multimedia documents accompanies the document while does not affect the usage of the document, but it can be extracted to authenticate the document [9] or demonstrate the copyright owner [10] or trace the traitor [11].

In the past several decades, many information hiding schemes and systems [12-27] have been proposed. These schemes or systems can be classified into single-purpose schemes [12-16] and multipurpose schemes [17-27]. Single-purpose schemes are designed to achieve one function. Robust schemes are mainly designed for multimedia copyright protection [12] or traitor tracing [13]. In copyright protection schemes, the robust watermark is the owner's logo. While in traitor tracing or source tracing schemes, the robust watermark is a fingerprint to denote the ID or identity of the traitor. Fragile schemes are mainly designed for content authentication [14]. Other schemes are designed for annotation [15] or secret transmission [16]. In recent years, many multipurpose schemes have been presented and most of them are double-purpose. Most schemes can fulfill both content authentication and copyright protection by embedding both a fragile watermark and a robust watermark [17-22]. Some robust schemes can fulfill two purposes by embedding two robust watermarks, one is visible for copyright notification and the other is invisible for copyright protection [23]. Some schemes are designed for both image retrieval and copyright protection [24] or content authentication [25]. Some schemes are designed for both secret communication and content authentication [26]. Some schemes can achieve three purposes, i.e., copyright protection traitor tracing and authentication by embedding the owner's copyright logo, the buyer's identity and a fragile watermark [27]. All these traditional multipurpose schemes were mainly designed for digital images, digital video and digital audio. Furthermore, there are few schemes considering how to embed multilevel fingerprints to trace multiple distribution processes. In addition, to the best of our knowledge, there are almost no multipurpose schemes designed for WORD files, PPT files, EXCEL files, WEB pages, PDF files or software codes. Although there are some single-purpose information hiding schemes designed for them [28-32], they mainly focus on how to hide information in these files, e.g., use annotation watermarks to manage the documents.

Based on above backgrounds, this paper presents a Multipurpose framework based on Multilevel Multichannel Information Hiding (MMMIH) in order to provide a more robust and conflict-prevented scheme with whole life cycle and full protection. This framework is developed for all kinds of multimedia documents, including images, video, audio, OFFICE documents, PDF files, database, software codes and WEB pages. This framework is developed to protect and/or authenticate and/or trace a multimedia document in its entire life time. This framework has been successfully applied in protecting and tracing Alibaba Group's documents.

The remainder of this paper is organized as follows. Section 2 proposes our MMMIH framework. Section 3 gives three example implementations of our framework. Section 4 evaluates the effectiveness of our framework based on the interfaces we developed and also compares the concrete algorithm we designed with existing watermarking schemes in terms of detection accuracy or qualitative analysis for a concrete application. Section 5 concludes the whole paper.

2. **The Proposed MMMIH Framework.** Our MMMIH framework consists of three kinds of modules, i.e., Watermark Embedding Module (WEM), Transmission Control Module (TCM) and Watermark eXtraction Module (WXM). Controlled by the embedding key, the WEM module embeds suitable watermarks in the original multimedia document or intermediate watermarked document (for multilevel embedding). According to the extraction key, the WXM module extracts watermarks from the received document to provide traitor IDs or authenticate the document or get the copyright logo or extra information related to the document. The TCM module involves the information appending mechanism, the embedding and extraction mechanism and the recognition and control mechanism. Each dash line means that the corresponding function or operation is optional. In order to make our framework work better as an organic whole, we define a Watermark Information Structure (WIS) to discriminate and recognize different watermarks and also provide some required control information for watermark extraction or further watermark embedding. Our contribution lies in four aspects. First, our framework is designed for multiple purposes, including copyright protection, content authentication, source tracing, annotation, secret communication, etc., and suitable for all kinds of multimedia documents, including images, video, audio, WORD files, PDF files, EXCEL files, PPT files, WEB pages, software codes, etc. Second, our framework can protect and/or authenticate and/or trace a multimedia document in its entire life time, and this framework has been successfully applied in protecting and tracing Alibaba Group's documents. Third, many novel techniques are proposed for data hiding in various documents. For example, we propose a novel technique that embedding one watermark in images and video achieves two purposes, i.e., copyright protection and content authentication, or source tracing and content authentication. Another example is to embed information in WEB pages based on dash lines. Finally, In order to make our framework work better as an organic whole, we define a watermark information structure to discriminate and recognize different watermarks and also provide some required control information for watermark extraction or further embedding. The whole block diagram of our MMMIH framework is shown in Figure 1, where WEM, WIS, TCM, WXM and WDI mean watermark embedding module, watermark information structure, transmission control module, watermark extraction module, watermark description information respectively. The detailed description is given in the following four subsections.

2.1. **The WIS structure.** Our framework can embed four kinds of watermarks in a multimedia document, i.e., copyright logo (copyright watermark), fragile watermark, fingerprints (tracing watermarks) and extra information (annotation watermark). The copyright logo is used to show the copyright owner. The fragile watermark is used to show which part of the document is tampered with. Fingerprints are used to trace several distribution processes. The extra information is used to record the date time or the watermark version or some other information to denote the allowed or forbidden operations on the document. In order to manage and discriminate these four types of watermarks, we adopt the WIS structure (see Figure 2), which mainly consists of four parts, i.e., prefix code, document type, watermark metadata, and watermark data. The prefix code is a

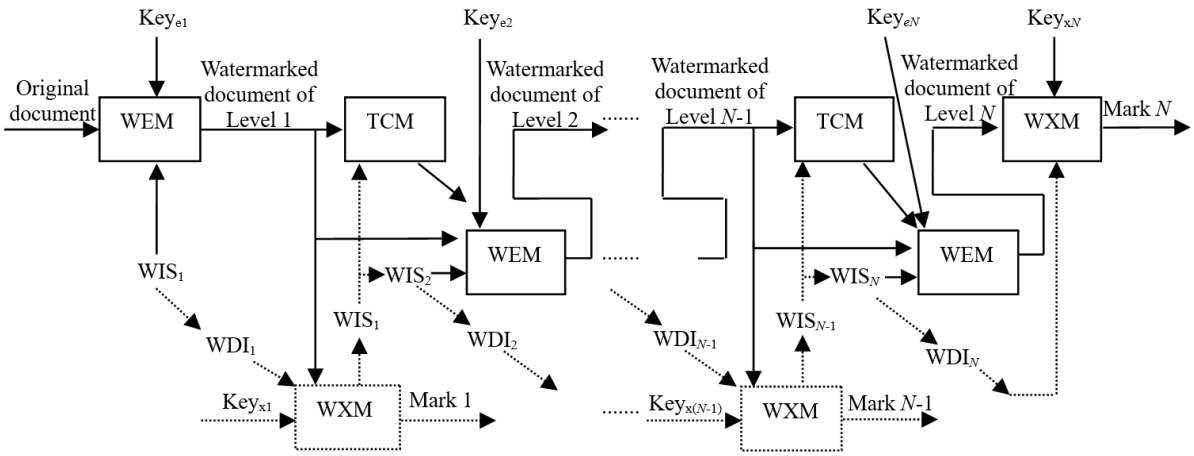


FIGURE 1. The whole block diagram of our MMMIH framework

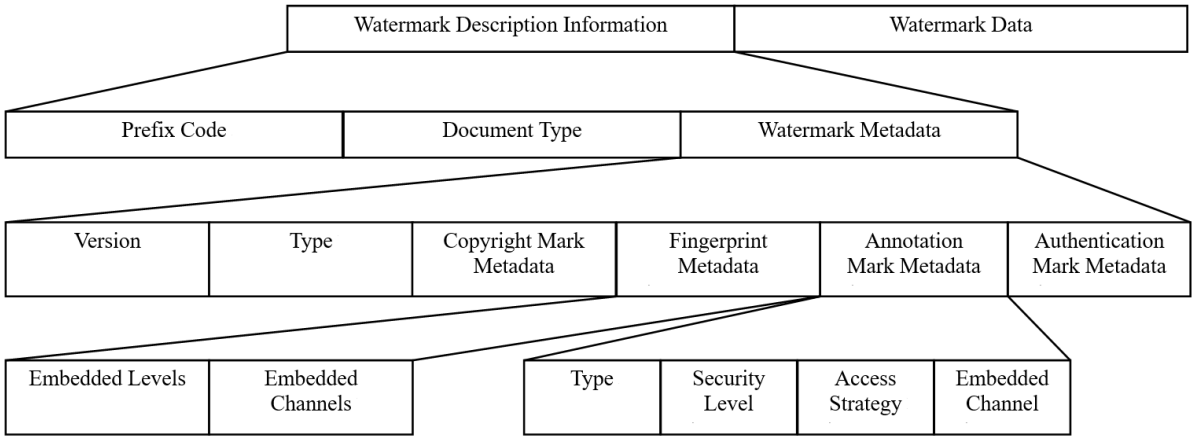


FIGURE 2. The proposed watermark information structure

two-byte code. The document type occupies one byte, where five bits denote the type (e.g., for image 00000, and for video 00001), one bit denotes the embedding capacity (high or low) and the remainder two bits are reserved.

The third part of the WIS structure consists of six subparts, including watermark version, watermark type, copyright watermark metadata, fingerprint metadata, annotation watermark metadata, authentication watermark metadata. The watermark version and the watermark type occupy one byte respectively. Currently, the first four bits in the watermark type denote which kinds of watermarks are embedded, e.g., 1010 means that there are copyright and annotation watermarks without fingerprints and authentication watermark. The copyright original metadata indicates the number of logos embedded, the information related to embedded channels (e.g., watermark lengths and embedding locations) and the number of redundant embedding times for each logo. The fingerprint metadata indicates the number of levels embedded, the information related to embedded channels (e.g., watermark lengths and embedding locations) and the number of redundant embedding times for each fingerprint. The annotation watermark (i.e., extra information) metadata includes the type of extra information, the security level, the access strategy, the information of embedded channel (e.g., watermark length and embedding location) and the number of redundant embedding times. The authentication watermark metadata includes the information of embedded channel (e.g., watermark length and embedding location) and the number of redundant embedding times.

The first three parts of the WIS structure can be viewed as a kind of extraction code, which can help us correctly extract the watermark information from the received document. The first three parts of the WIS structure can be also used as a control code to determine if the received document can be further transmitted to other persons or embedded with another watermark or not. Therefore, we define the first three parts of the WIS structure as Watermark Description Information (WDI) as given in Figure 2. The fourth part of WIS, i.e., the watermark data, may be a file to be embedded into the document. In this case, WIS is just WDI without watermark data since the data is in a file.

2.2. **The WEM module.** The WEM module is used to embed suitable watermarks into the original or received intermediate document according to the embedding key. The general block diagram is shown in Figure 3. There are possible three or four input signals. For the original document, the TCM module is not used. For the received document, the TCM module will give some additional information to determine how to embed the watermark or refuse to embed the watermark. The WEM module embeds the watermark data in the WIS structure into the original or received document according to both the key $\text{Key}_{e,i}$ and the WDI information in the WIS structure, generating the watermarked document of Level i.

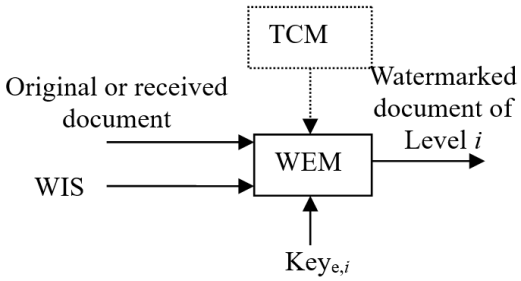


FIGURE 3. The general watermark embedding module

To explain the embedding module more clearly, we give a multichannel watermark embedding example as shown in Figure 4 and Figure 5. Figure 4 shows the generation diagram of the multichannel WDI. Figure 5 shows two possible embedding schemes to embed the WDI and the watermark data redundantly. In Case 1, Channel 1 is used to

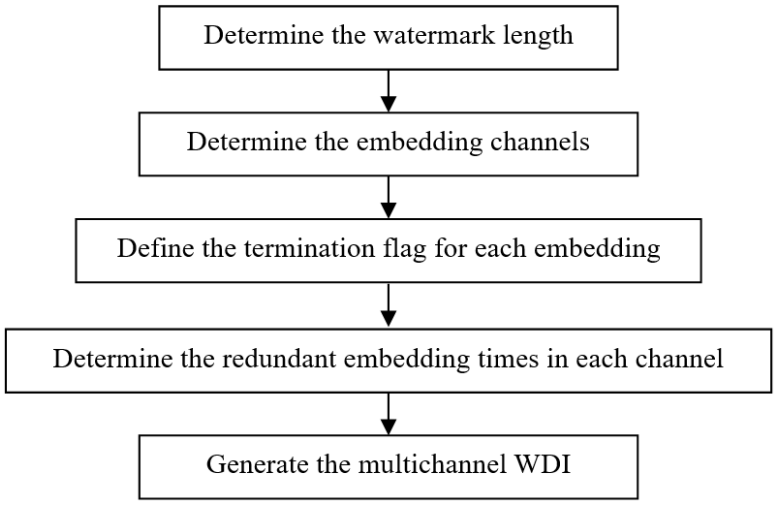


FIGURE 4. The generation process of the multichannel WDI

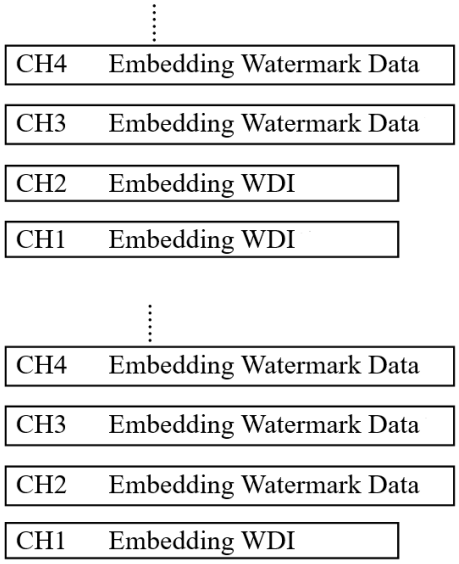


FIGURE 5. Two example cases for multichannel embedding

embed the WDI, Channels 2-4 are used to embed the watermark data redundantly. In Case 2, Channels 1-2 are used to embed the WDI redundantly, and Channels 3-4 are used to embed the watermark data redundantly. In fact, the WDI can be stored in a file for later use to avoid the fact that the embedded WDI may be lost if the watermarked document suffers attacking.

2.3. **The WXM module.** The WEM module is used to extract watermarks from the suspect watermarked document. The general block diagram is shown in Figure 6. There are possible three input signals, i.e., the suspect document or the received document from Level i, the WDI from Level i (e.g., the extraction code saved in a file) and the extraction key $\text{Key}_{x,i}$. There are two possible output signals, i.e., the extracted mark and the extracted WSI which was formerly embedded in the document. This extracted WSI is used by the TCM module to control the watermark embedding process for next level.

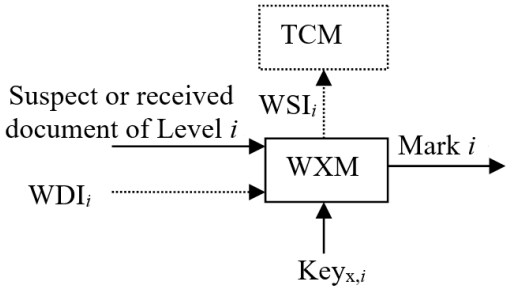


FIGURE 6. The general watermark extraction module

2.4. **The TCM module.** The TCM module is used to control the watermark embedding process according to the extracted information from the previous level. The general block diagram is shown in Figure 7. There are possible two input signals, i.e., the received document from Level i, the WDI extracted from Level i or the WDI (extraction code) saved in a file. There is one output signal to control the WEM module. The TCM module first calls the WXM module to extract the watermark information which has been embedded in the document. Based on the extracted information and other input information, the

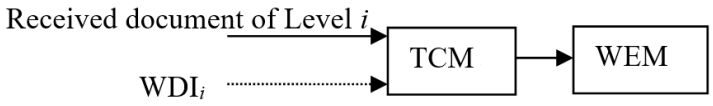


FIGURE 7. The general transmission control module

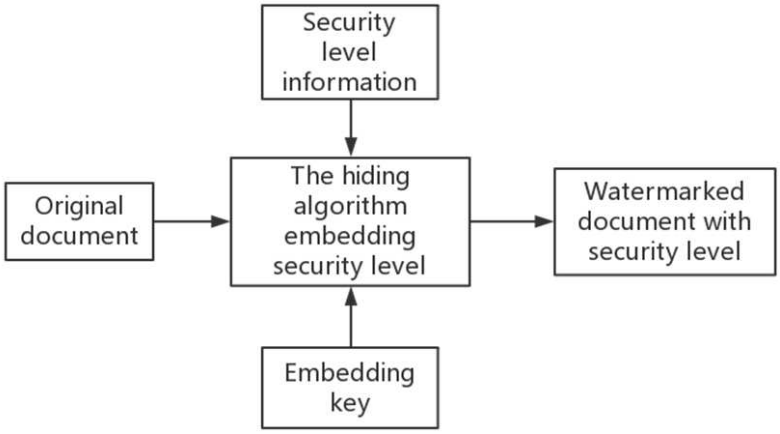


FIGURE 8. The annotation watermark embedding example

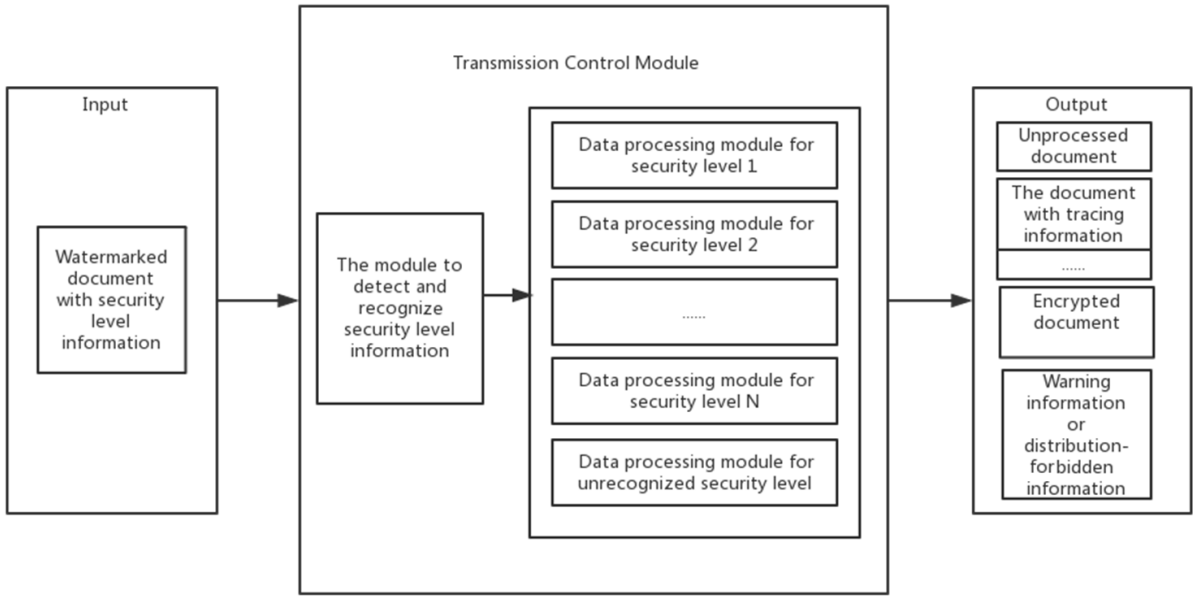


FIGURE 9. The general transmission control module

TCM module determines how to do in the next step, e.g., TCM may also call the WEM module to embed another input fingerprint to trace another possible traitor.

To explain the transmission module more clearly, we give an annotation watermark embedding example as shown in Figure 8 and Figure 9. Figure 8 views the security level as the annotation watermark and embeds it (maybe together with the copyright logo) into the original document according to the embedding key, generating a watermarked document which is embedded with the security level information. Figure 9 shows how the TCM controls the subsequent operations. The input is the suspect watermarked document, and the TCM module calls the WXM module to extract the watermark data (i.e., the security level information). If the security level is extracted successfully, then

it will drive the document data processing for the corresponding security level. The processed document is then input into the WEM module and embedded with the suitable watermark to output corresponding watermarked document or even encrypted document for high security level. If no security level is extracted, then the document remained unchanged. If the security level is annotated with "forbidden", then the document is forbidden to be distributed any longer. If the security level is annotated with "warning, one distribution only", then the document is only allowed to be distributed for one time.

2.5. **Key techniques involved in our framework.** In our framework, there are three key techniques. The first technique is how to embed multiple watermarks during the life cycle of the document. The main issue is that the later embedded watermark may affect the former embedded watermarks. For audiovisual documents, our main solution is to adopt different transform coefficients to embed different watermarks. For OFFICE files and PDF files, we find different redundant parts or different images in documents (many OFFICE files or PDF files typically contain some images) to embed different watermarks.

The second key technique is how to embed one watermark with two purposes. This is one of our main contributions. Our solution is to embed a tiled watermark which is composed of small logos. Thus, a part of watermarked image is tampered with, then the corresponding part of the extracted watermark will be lost, and we can know that this part has been modified by someone. On the other hand, because only small part is modified, from the overall extracted watermark, we can still see the logos clearly. Thus, by averaging over all tiled logos, we can extract the final logo to clarify the copyright.

The third technique is how to quickly check if a document has been embedded with some watermarks (and thus we can embed following watermarks in other places in order not to affect the formerly embedded watermarks). Our solution is to design a watermark information structure as described in Section 2.1. We can easily extract the prefix code and the watermark type from the suspect watermarked document.

3. **Example Implementations.** In this section, we give three example implementations to show how our framework works. These two implementations are performed for images WEB pages and PPT files respectively. The detailed descriptions are given in the following three subsections.

3.1. **Multipurpose multilevel multichannel information hiding for images.** Images are common multimedia documents used broadly in our everyday life. Sometimes, an image is a work of art, which has value and should be protected. Sometimes, an image is a digital certificate that should be authentic. In addition, leaking sensitive information via transmitting screenshots over mobile instant messaging has become a serious and urgent problem to be solved. Thus, developing a multipurpose multilevel multichannel information hiding scheme for images is very useful. This scheme can be used to protect the copyright of an image and authenticate this image and also trace the distribution of this image at the same time.

We developed an interface to simulate the MMMIH framework for images. This interface consists of four parts, i.e., original image input module, original watermark input module, watermarked image output module, extracted watermark output module. The "browse" button is used to select files, while the "Save as" button is used to save files or results. The "information" edit control is used to display the related information, e.g., the image file path, the image size, PSNR and NC values. The "Original Image" control is used to display the opened original image or intermediate watermarked image. The "Original Watermark" controls display all kinds of watermarks including robust watermark, fragile watermark, Level 1 fingerprint, Level 2 fingerprint, Level 3 fingerprint

and extra information. One of merits of our framework is that we can achieve multilevel multichannel embedding, i.e., watermarks in different levels are independent since they are embedded into different locations (channels). The "embed mode" or "extract mode" can be selected in the set {CP, CA, CPCA, FP1, FP2, FP3} which means copyright watermark (may be with extra information) only, authentication watermark only, both copyright and authentication watermarks, fingerprint Level 1, fingerprint Level 2 and fingerprint Level 3 respectively. While pressing the "Embed" or "Extract" button, there will be a dialog to determine the embedding parameter or input the extraction code and passwords. The "Watermarked Image" control is used to display the watermarked image or opened a suspect image.

To achieve different purposes simultaneously, we should select a suitable core embedding algorithm that can realize the multichannel embedding. As we know, image watermarking algorithms proposed so far can be divided into two main groups: those which embed the watermark directly in the spatial domain [5,16,33] and those operating in a transformed domain, e.g., the frequency domain [12,14,34,35]. In our framework, considering the time complexity, we adopt QIM [33] in the DCT domain with special pre-processing steps as our robust watermarking algorithm to make it robust to scaling and JPEG compression operations. The robust watermark embedding algorithm can be expressed as follows.

Step 1: The original image is resized into a fixed width W (e.g., $W = 512$) preserving the aspect ratio based on linear interpolation. This step is an essential step to achieve the scaling-resilience performance.

Step 2: The Y component of the original image is segmented into non-overlapping blocks of size 8×8.

Step 3: The integer DCT is performed on each block to obtain 64 coefficients. Scan these coefficients in the zigzag manner and select two mid-frequency coefficients to embed watermark bits for each level. That is, each block can be embedded with 2 watermark bits for each level. To embed four levels, we need 8 different DCT coefficients.

Step 4: The watermark bits are sequentially embedded into DCT blocks using the dither modulation technique [33]. These watermark bits can be redundantly embedded with multiple times as long as there are enough DCT blocks to be embedded in order to achieve the best robustness.

Step 5: Perform the inverse transform on these watermarked DCT blocks, we can obtain the watermarked image and then resize it into its original size to get the final watermarked image.

The fragile watermark embedding is also based on DCT domain by modifying another four coefficients using mod operations. This method can be used to locate the tampering locations.

In our framework, different levels are independent because they adopt different coefficients. Before extraction, we also need to pre-process the suspect image, i.e., the suspect image should be resized into a fixed width W (e.g., $W = 512$) preserving the aspect ratio based on linear interpolation. Therefore, one of merits of our robust method is that it can resist the composite attack of scaling and low quality factor JPEG compression.

3.2. **Multipurpose multilevel multichannel information hiding for WEB pages.** Growths of Internet use and copy culture present a challenge for copyrights of original information on web. Different methods have been studied for multimedia objects but few are available for securing textual information without altering its integrity. Web based attacks have been a very common practice in recent years and hence need strong security mechanisms for the sake of secret communication. Besides other data types available on web, text is the most dominant part and is of utmost importance of securing it. Therefore,

it is urgently required to have rights protection solutions which remain attached to the text even if it is re-produced, edited, and modified. Text watermarking [31,36,37] is one of the most effective methods for digital document protection. In our framework, we can achieve protection and fingerprinting purposes by using four-level independent watermark embedding in a WEB page.

The interface for WEB pages is similar to the interface for images as shown in Figure 10. The interface consists of four parts, i.e., original WEB file input module, original watermark input module, watermarked WEB file output module, extracted watermark output module. The "browse" button is used to select files, while the "Save as" button is used to save files or results. The "information" edit control is used to display the related information, e.g., the WEB file path, the NC values. The "Original WEB" control is used to display the opened original WEB file or intermediate watermarked WEB files. The "Original Watermark" controls display all kinds of watermarks including robust watermark, Level 1 fingerprint, Level 2 fingerprint, Level 3 fingerprint and extra information. One of merits of our framework is that we can achieve multilevel multichannel embedding, i.e., watermarks in different levels are independent since they are embedded into different properties (channels). The "embed mode" or "extract mode" can be selected in the set {CP, FP1, FP2, FP3} which means copyright watermark (may be with extra information), fingerprint Level 1, fingerprint Level 2 and fingerprint Level 3 respectively. While pressing the "Embed" or "Extract" button, there will be a dialog to determine the embedding parameter or input the extraction code and passwords. The "Watermarked WEB" control is used to display the watermarked WEB or opened suspect WEB file.

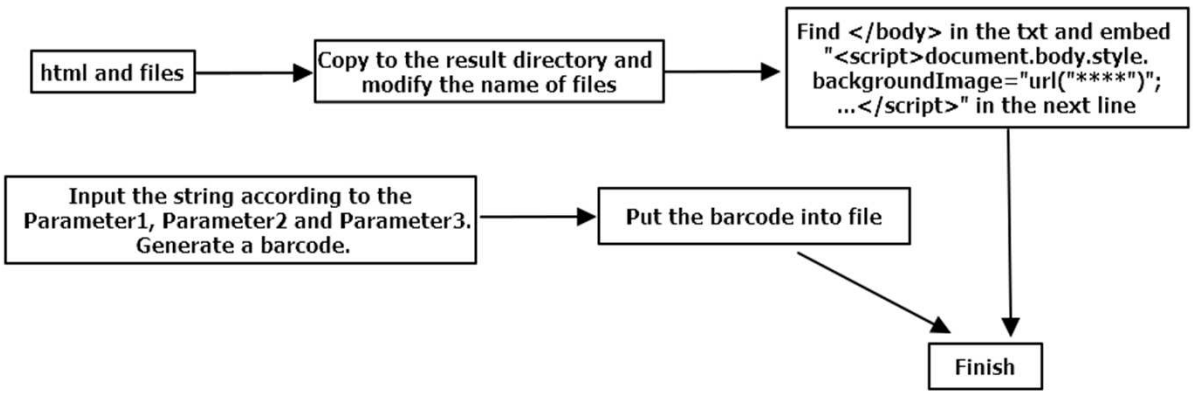


FIGURE 10. The embedding strategy of Method 9 for WEB pages

Most of the methodologies studied for digital text watermarking depend on the content itself and do not address the medium. Web watermarking addresses the issue of protecting not only the content but the carrying medium itself by taking the construction elements of the page into mind. In our framework, we design nine embedding algorithms for WEB pages, which are 1) embedding watermarks in the images of the WEB page based on DCT domain; 2) embedding watermarks in the script annotations; 3) embedding watermarks in the webpage's script div (in the attribute: display:none); 4) embedding watermarks in the js script; 5) weightedly mixing watermark image and the images in the webpage; 6) embedding inversely-colored watermark images into webpage's background and tiling; 7) embedding strings in webpage's background and tiling (using canvas brush); 8) embedding inversely-colored QR codes into webpage's background and tiling; 9) embedding the bar code horizontally (or vertically) in webpage's background and horizontally (or vertically) tiling. For example, the method to embed the bar code horizontally (or vertically) in webpage's background and horizontally (or vertically) tiling can be shown in Figure 10.

3.3. **Multipurpose multilevel multichannel information hiding for PPT files.** Multimedia courseware is an important resource in the network teaching system. However, while they bring great convenience to people, they also bring about copyright disputes caused by illegal piracy and malicious tampering. With the spread of the Internet, if you do not take precautions, PPT files can easily be taken by others. In view of the increasingly serious infringement problem, it is of considerable practical significance to study how to effectively protect the copyright of multimedia courseware. Nowadays, there are few articles and researches on watermarking of PPT documents, and there is almost no invisible watermark part of PPT documents. The invisible digital watermarking method for PPT documents in this article is relatively advanced and practical. Many articles about word document watermarking can be found through paper retrieval. Most of the research methods focus on modifying the text size, size and other attributes to embed the watermark information. Its form is single and it is not resistant to format brushing attacks. However, these methods have given us a lot of inspiration, allowing us to expand new methods from different perspectives, and rationally use the unique components in PPT to embed watermarks, which ensures the security and improves the robustness of watermarks.

The interface for PPT files is similar to the interface for images and WEB pages. The interface consists of four parts, i.e., original PPT file input module, original watermark input module, watermarked PPT file output module, extracted watermark output module. In our framework, we design six embedding algorithms for PPT files as follows. 1) Embed an invisible rectangular frame in PPT, in which the encrypted information is put. 2) Embed information in images involved in PPT, i.e., selecting the appropriate image carrier, and embed the information in the DCT coefficients of the carrier image (e.g. dither modulation algorithm). 3) Embed in font sizes, i.e., information is embedded by modifying the size of the font in the text box, and the font size is changed by 0.5. 4) The purpose of embedding information is achieved by adjusting the automatic rotation number of the font, and the automatic rotation number is 0 or -1 according to the watermark bit. 5) The embossed effect of the font is adjusted to achieve the purpose of embedding information, and the embossed effect is controlled by the watermark bit. 6) Information embedding is completed by searching keywords, and synonyms are replaced for keywords, where different words represent different 0/1 information.

For example, the algorithm principle for Method 2 is as follows: Select up to 40 images with sufficient embedding positions in PPT, and embed the information. The information is redundantly embedded 3 times in each image (at least 1 time), and the information header is used to identify the embedded picture in the embedded information, so adding or deleting pictures in the PPT will not affect the extraction. In the extraction process, select the first 9 images with information headers (the largest odd number is taken if there are less than 9 images), and after the information is extracted, average statistics are used to restore the original embedded information.

4. **Results and Discussion.** In order to test the effectiveness of the proposed framework, we adopt three kinds of multimedia to develop corresponding simulation interfaces. The three types of multimedia are images, WEB pages and PPT files. Based on the MMMIH interface for images, we can browse an image and embed different kinds of watermarks into the image by changing the embedding mode, and three fingerprints can serve as three-level traitor tracing. We can also browse a suspect image (which may suffer attacking) and extract the corresponding watermark based on the extraction code. In our MMMIH system for image copyright protection, we design a robust image watermarking scheme in the DCT domain named Scaling-Resilience Quantization Index Modulation

with Template Patterns (SRQIMTP) as given in Section 3.1. Based on this robust watermarking algorithm, a four-level watermarking example for images is shown in Figures 12-14. The four levels include a copyright watermark and three fingerprints. Figure 12 shows the original image, the original robust watermark and three fingerprints respectively. Figure 13 shows the four level watermarked images with PSNR values 40.25dB, 38.38dB, 37.15dB and 36.05dB respectively. To show the superiority of our SRQIMTP scheme (one level embedding) under the composite "scaling + JPEG compression" attack (QF = 70 JPEG compression together with reducing into 2/3 original size), based on 10 512×512 test images, we compare it with other three schemes, i.e., original QIM [33], Ali

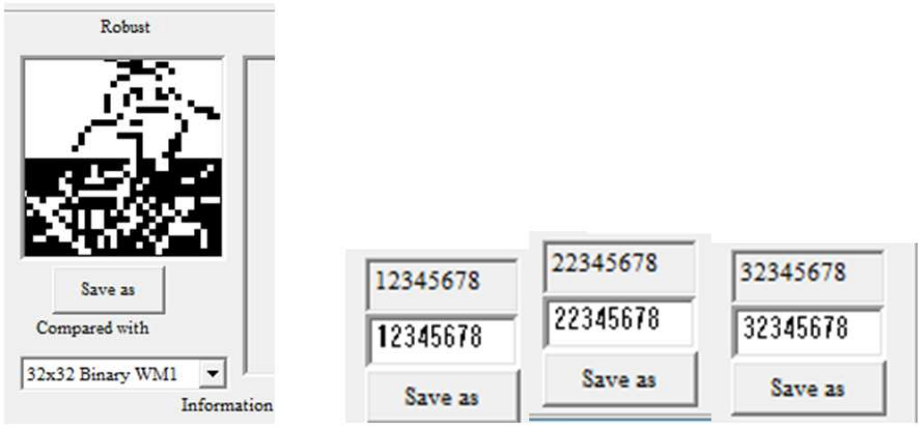
FIGURE 11. The embedding strategy of Method 2 for PPT files

(a) Original image (b) Robust watermark (c) Three fingerprints

FIGURE 12. Original image and four watermarks to be embedded

(a) With robust mark (b) Further with Level 1 fingerprint (FP) (c) Further with Level 2 FP (d) Further with Level 3 FP

FIGURE 13. Four-level watermarked images



(a) Extracted robust watermark

(b) Extracted fingerprints

FIGURE 14. Four extracted watermarks (NC = 1.0) under no attack

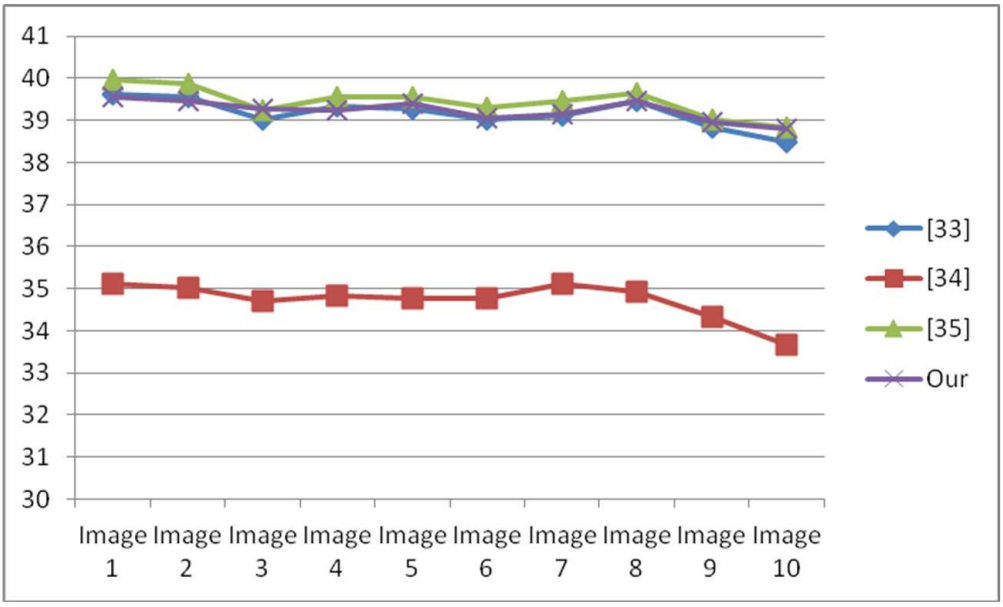


FIGURE 15. Comparisons of PSNR of the watermarked image (Y component)

et al.'s [34] in 2014 and Moosazadeh and Ekbatanifard's [35] in 2017, in terms of PSNR of the watermarked image (Y component), successful detection or not after composite attack (0 denotes fail, 1 means success) and the embedding time complexity (compared with our scheme) in Figures 15-17 respectively. Furthermore, several attacks have been tested over 1000 images and the comparison results among several embedding schemes are shown in Table 1. From these results, we can see that our method is better than existing schemes.

Secondly, we test the effectiveness of our MMMIH framework for WEB pages, where we embed different watermarks independently in different properties of the WEB page, i.e., multichannel embedding mode. We give Method 9 in Section 3.2 as an example, Figure 18 shows the bar code generated from the information to be embedded "Alibaba", and this bar code is embedded as a dash line in the WEB page as shown in Figure 19. Thus, based on the bar code, even the WEB page is made a screenshot, we can also recognize

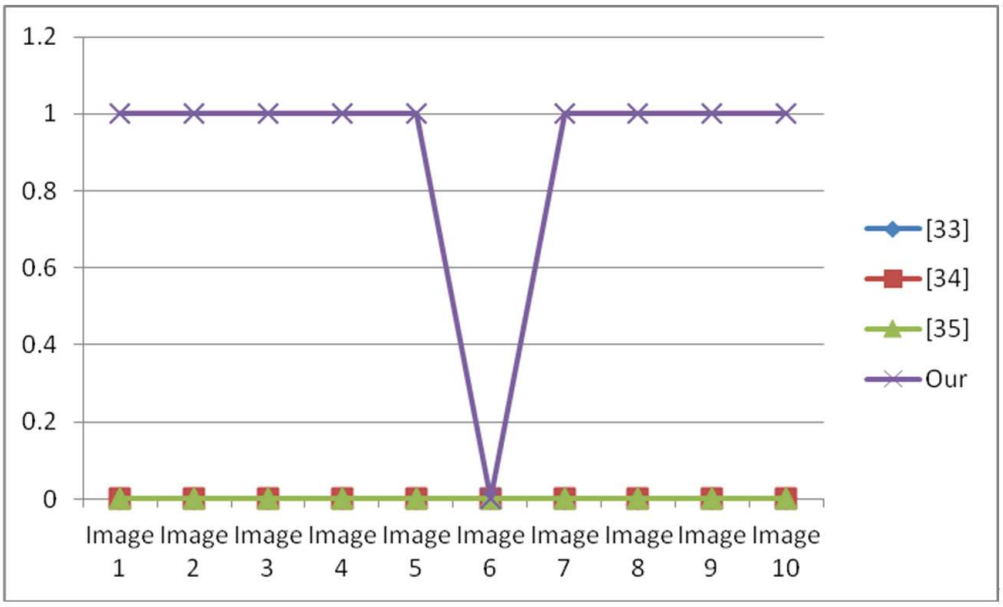


FIGURE 16. Successful detection or not after composite attack (0 denotes fail, 1 means success)

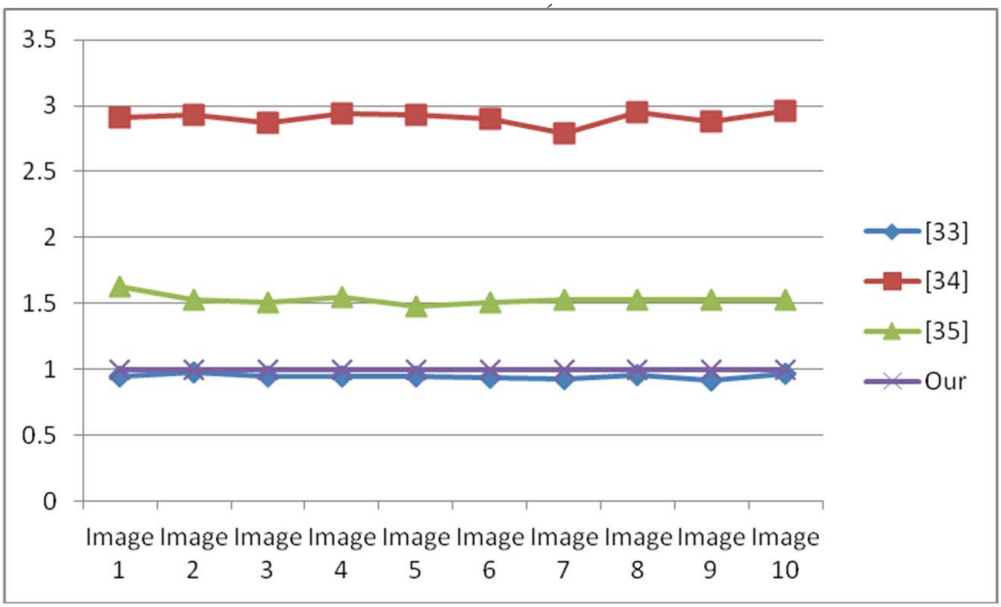


FIGURE 17. Comparisons of embedding time complexity (compared with our scheme)

the bar code. Table 2 compares this scheme with two existing schemes. From this table, we can see that our scheme performs better than existing schemes.

Finally, we also test the effectiveness of our MMMIH framework for PPT files, where we embed different watermarks independently in images containing in the PPT file, i.e., we give Method 2 in Section 3.3 as an example. Figure 20 shows three original slices of a sample PPT (totally 40 slices with images) and the corresponding watermarked slices of the PPT. We can see that the watermark is invisible in PPT slices, where the average PSNR of images is 36dB with four level watermarks. Table 3 shows the advantage of our scheme under various attacks. From these results, we can see that our scheme can embed enough information in PPT since there are often many pictures embedded in a PPT file,

TABLE 1. Comparisons of our scheme with other three schemes in terms of detection accuracy under different attacks

Method	[33]	[34]	[35]	Our
JPEG (QF = 80)	100%	100%	100%	100%
JPEG (QF = 60)	99.6%	99.9%	100%	99.9%
Scaling to 3/4 original size	0	0	0	100%
Scaling to 1/2 original size	0	0	0	99.8%
Gaussian filtering ($\sigma = 1$)	99.7%	95.1%	99.7%	99.7%
Cropping left-upper corner	100%	99.9%	85%	100%
Median filtering (3×3)	99.5%	99.3%	99.5%	99.6%

FIGURE 18. The generated bar code from "Alibaba"

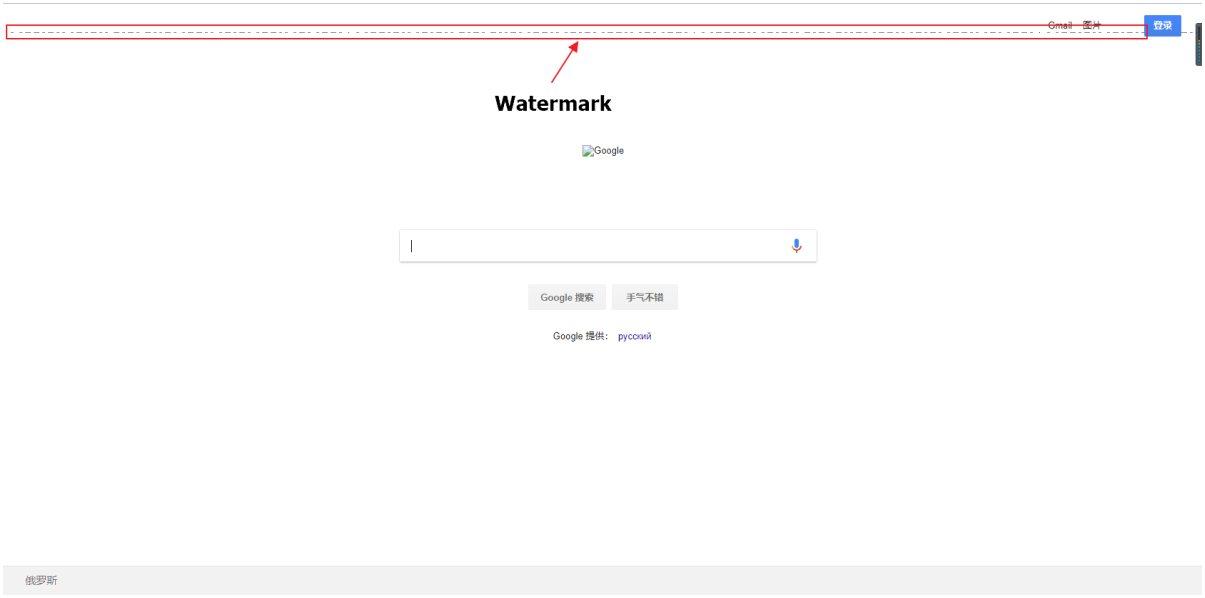
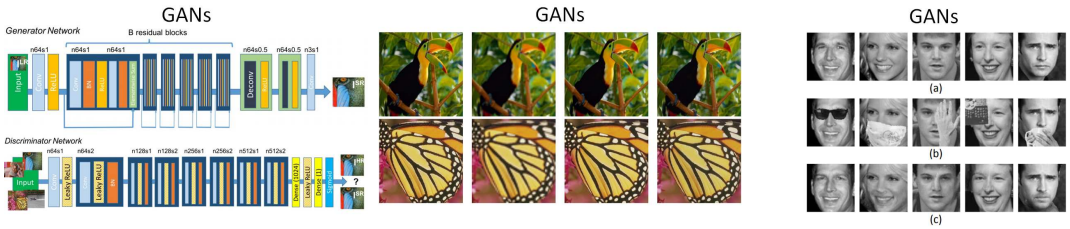


FIGURE 19. The watermarked WEB page with a bar code

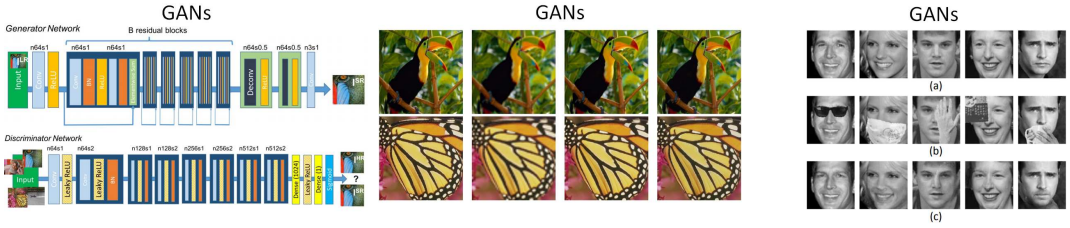
TABLE 2. Comparisons of our WEB page watermarking scheme with other two schemes

Method	Invisible	Anti-Copy	Anti-Screenshot	Anti-Photocopy
[36]	yes	yes	no	no
[37]	yes	yes	no	no
Our	yes	yes	yes	yes

and our scheme is robust enough since as long as there is a picture left in the PPT we can extract the watermark.



(a) Original three slices



(b) Watermarked three slices

FIGURE 20. Original slices and the corresponding watermarked slices of the sample PPT

TABLE 3. Performance of our PPT information hiding scheme

Attack	Watermark extraction
Convert PPT to PPTX	success
Convert PPTX to PPT	success
5 slices are randomly selected and removed from PPT	success
All slices with images are removed from PPT	fail
Modify the text in the PPT	success
Add slices into the PPT with images	success

5. **Conclusions.** This paper presents a general multipurpose multilevel multichannel information hiding framework for all kinds of documents. This framework can fulfill multiple purposes including copyright protection, content authentication, traitor tracing, document security management and so on. The multilevel or multichannel embedding schemes can be used to fulfill these multiple purposes. From all simulation results, we can see that our framework can embed multiple watermarks and can extract all watermarks correctly and independently. Furthermore, we also have much better core algorithms than existing schemes. Future work will concentrate on further improving the framework structure and improving the performance and security by combining the information hiding scheme with other techniques. We will also promote our framework to the field of video surveillance and evidence anti-tampering [38,39].

Acknowledgement. This research is supported in part by the National Key Research and Development Program of China under Grant No. 2020AAA0140004 and the Public Good Research Project of Science and Technology Program of Zhejiang Province under Grant No. LGG21F020005.

REFERENCES

[1] J. Ding and A. Petzoldt, Current state of multivariate cryptography, *IEEE Security and Privacy*, vol.15, no.4, pp.28-36, 2017.

[2] D. He, S. Zeadally, N. Kumar and W. Wu, Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures, *IEEE Trans. Information Forensics and Security*, vol.11, no.9, pp.2052-2064, 2016.

[3] D. Butin, Hash-based signatures: State of play, *IEEE Security and Privacy*, vol.15, no.4, pp.37-43, 2017.

[4] A. A. Yavuz, A. Mudgerikar, A. Singla, I. Papapanagiotou and E. Bertino, Real-time digital signatures for time-critical networks, *IEEE Trans. Information Forensics and Security*, vol.12, no.11, pp.2627-2639, 2017.

[5] R. G. van Schyndel, A. Z. Tirkel and C. F. Osborne, A digital watermark, *Proc. of the 1st IEEE International Conference on Image Processing*, Austin, TX, USA, pp.86-90, 1994.

[6] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Processing*, vol.6, no.12, pp.1673-1687, 1997.

[7] S. Xiang and J. He, Database authentication watermarking scheme in encrypted domain, *IET Information Security*, vol.12, no.1, pp.42-51, 2018.

[8] J. R. Mahajan and N. N. Patil, Alpha channel for integrity verification using digital signature on reversible watermarking QR, *Proc. of IEEE International Conference on Computing Communication Control and Automation*, Pune, India, pp.602-606, 2015.

[9] A. S. Bhaisare, A. H. Karode and S. R. Suralkar, Implementation of real time digital watermarking system for video authentication using FPGA, *Proc. of IEEE International Conference on Global Trends in Signal Processing, Information Computing and Communication*, pp.358-362, 2016.

[10] R. D. Shelke and M. U. Nemade, Audio watermarking techniques for copyright protection: A review, *Proc. of IEEE International Conference on Global Trends in Signal Processing, Information Computing and Communication*, pp.634-640, 2016.

[11] J. Abraham and V. Paul, A blind watermarking method for fingerprinting digital images, *Proc. of IEEE International Conference on Data Mining and Advanced Computing*, Ernakulam, India, pp.145-149, 2016.

[12] S. P. Vaidya and P. V. S. S. R. C. Mouli, Adaptive digital watermarking for copyright protection of digital images in wavelet domain, *Procedia Computer Science*, vol.58, pp.233-240, 2015.

[13] F. Chaabane, M. Charfeddine and C. B. Amar, A multimedia tracing traitors scheme using multi-level hierarchical structure for Tardos fingerprint based audio watermarking, *Proc. of IEEE International Conference on Signal Processing and Multimedia Applications*, Vienna, Austria, pp.289-296, 2014.

[14] X. Qi and X. Xin, A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization, *Journal of Visual Communication and Image Representation*, vol.30, pp.312-327, 2015.

[15] Y.-H. Yu and C.-C. Chang, A high capacity reversible data hiding scheme for annotation, *Proc. of the 2nd IEEE International Symposium on Intelligent Information Technology Application*, Shanghai, China, pp.940-944, 2008.

[16] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho and K. H. Jung, Image steganography in spatial domain: A survey, *Signal Processing: Image Communication*, vol.65, pp.46-66, 2018.

[17] C. S. Lu and H. Y. M. Liao, Multipurpose watermarking for image authentication and protection, *IEEE Trans. Image Processing*, vol.10, no.10, pp.1579-1592, 2001.

[18] Z.-M. Lu, D.-G. Xu and S.-H. Sun, Multipurpose image watermarking algorithm based on multistage vector quantization, *IEEE Trans. Image Processing*, vol.14, no.6, pp.822-831, 2005.

[19] N. Chen and J. Zhu, Multipurpose speech watermarking based on multistage vector quantization of linear prediction coefficients, *The Journal of China Universities of Posts and Telecommunications*, vol.14, no.4, pp.64-69, 2007.

[20] C. Zhang, L.-L. Cheng, Z. Qiu and L.-M. Cheng, Multipurpose watermarking based on multiscale curvelet transform, *IEEE Trans. Information Forensics and Security*, vol.3, no.4, pp.611-619, 2008.

[21] I. A. Ansari and M. Pant, Multipurpose image watermarking in the domain of DWT based on SVD and ABC, *Pattern Recognition Letters*, vol.94, pp.228-236, 2017.

[22] S. Kiani and M. E. Moghaddam, A multi-purpose digital image watermarking using fractal block coding, *Journal of Systems and Software*, vol.84, no.9, pp.1550-1562, 2011.
[23] Z.-M. Lu, H.-T. Wu, D.-G. Xu and S.-H. Sun, A multipurpose image watermarking method for copyright notification and protection, *IEICE Trans. Information and Systems*, vol.E86-D, no.9, pp.1931-1933, 2003.
[24] Z.-M. Lu, H. Skibbe and H. Burkhardt, Image retrieval based on a multipurpose watermarking scheme, *Lecture Notes in Artificial Intelligence*, vol.3682, pp.573-579, 2005.
[25] Z.-M. Lu, C.-H. Liu and H. Wang, Image retrieval and content integrity verification based on multipurpose image watermarking scheme, *International Journal of Innovative Computing, Information and Control*, vol.3, no.3, pp.621-630, 2007.
[26] Z.-M. Lu and S.-Z. Li, Multipurpose watermarking algorithm for secret communication, *Chinese Journal of Electronics*, vol.15, no.1, pp.79-84, 2006.
[27] Z.-M. Lu, Y.-N. Li, H.-X. Wang and S.-H. Sun, Multipurpose video watermarking algorithm in the hybrid compressed domain, *IEE Proceedings – Information Security*, vol.153, no.4, pp.173-182, 2006.
[28] R. A. Alotaibi and L. A. Elrefaei, Utilizing word space with pointed and un-pointed letters for Arabic text watermarking, *Proc. of UKSim-AMSS the 18th IEEE International Conference on Computer Modelling and Simulation*, Cambridge, UK, pp.111-116, 2016.
[29] J. Sun, Y. Fujii, H. Takebe, K. Fujimoto and S. Naoi, An image based watermark string detection system for document security checking, *Proc. of the 8th IAPR International Workshop on Document Analysis Systems*, Nara, Japan, pp.43-50, 2008.
[30] S. G. R. Ekodeck and R. Ndoundam, PDF steganography based on Chinese Remainder Theorem, *Journal of Information Security and Applications*, vol.29, pp.1-15, 2016.
[31] Q. Zhao and H. Lu, PCA-based web page watermarking, *Pattern Recognition*, vol.40, no.4, pp.1334-1341, 2007.
[32] M. D. Preda and M. Pasqua, Software watermarking: A semantics-based approach, *Electronic Notes in Theoretical Computer Science*, vol.331, no.20, pp.71-85, 2017.
[33] B. Chen and G. W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, *IEEE Trans. Information Theory*, vol.47, no.4, pp.1423-1443, 2001.
[34] M. Ali, C. W. Ahn and M. Pant, A robust image watermarking technique using SVD and differential evolution in DCT domain, *Optik*, vol.125, no.1, pp.428-434, 2014.
[35] M. Mohammad and E. Gholamhossein, An improved robust image watermarking method using DCT and YCoCg-R color space, *Optik*, vol.140, pp.975-988, 2017.
[36] N. Mir, Copyright for web content using invisible text watermarking, *Computers in Human Behavior*, vol.30, pp.648-653, 2014.
[37] R. J. Jaiswal and N. N. Patil, Implementation of a new technique for web document protection using unicode, *Proc. of the IEEE International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, India, pp.69-72, 2013.
[38] Y. Shin, M. Kim, K.-W. Pak and D. Kim, Practical methods of image data preprocessing for enhancing the performance of deep learning based road crack detection, *ICIC Express Letters, Part B: Applications*, vol.11, no.4, pp.373-379, 2020.
[39] E. P. Putra, S. Michael, T. O. Wingardi, R. L. Tatulus and W. Budiharto, Smart traffic light model using deep learning and computer vision, *ICIC Express Letters*, vol.15, no.3, pp.297-305, 2021.