International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.9 (2016), pp.29-38
http://dx.doi.org/10.14257/ijmue.2016.11.9.04

A Characteristic-Preserving Steganographic Method Based on Revision Identifiers

Lingyun Xiang[1,2], Caixia Sun[1,2], Niandong Liao[1,2] and Weizheng Wang[1,2]

1Hunan Provincial Key Laboratory of Intelligent Processing of Big Data on Transportation, Changsha University of Science and Technology, Changsha 410114, Hunan Province, China
2School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, Hunan Province, China
xiangly210@163.com

Abstract

Since the majority of the available steganographic schemes in OOXML format documents suffered the disadvantages of unsatisfactory anti-detection capability and security level, a characteristic-preserving steganographic method with high security is proposed in this paper. The proposed method embeds secret information by replacing the last three bytes of the values of the revision identifiers in the main document body of the OOXML format document, while preserving the normal characteristics of the document. Meanwhile, position marks are added to track the locations of the embedded information. In order to keep the internal data consistency of the document, the newly created values are added into other related parts. Experimental results show that the method not only possesses good imperceptibility and anti-detection capability, but also has high security and large embedding capacity.

Keywords: *Steganography; OOXML; Revision identifier; Anti-detection; Characteristic-preserving*

1. Introduction

Steganography is the art and science that aims to embed secret information into cover media objects imperceptibly for the purpose of covert communication and privacy protection [1]. The result of steganography is so-called stego object. The authorized receiver can be extracted the embedded secret information from the received stego object, which is transmitted on insecure channel without raising suspicion of an adversary. At present, most of the researches focus on the steganography using such cover media objects as images, videos and audios [2-4]. There are relatively few researches devoted to text documents especially the OOXML format documents.

As we all know, Microsoft Office documents are among the most popular electronic document types. They have been employed by an increasing number of users thanks to their rich features and ease of use. Now all Microsoft Office 2007-2015 documents adopt a new format which is called Office Open XML(OOXML) [5]. The appearance of the new format has attracted the attention of many researchers to engage information hiding for this type of documents. Related researches were introduced as follows.

Bora Park *et al.* [6] proposed a method for hiding information in OOXML format documents by using unknown parts and unknown relationships. The method has strong robustness but weak anti-detection capability because it can be detected by inspecting for the unknown parts and relationships. Zhangjie Fu *et al.* [7] proposed a steganographic method with better imperceptibility by splitting up the printable text, which is defined in the main part of the OOXML format document. The number of printable words contained in each segment represents the secret information. Simson L. Garfinkel *et al.* [8] proposed to use encryption and the comment feature of ZIP archive and XML files to hide information in OOXML format documents. Unfortunately, the inserted comments would be discarded when the document is rewritten. The method for information hiding by replacing the values of the revision identifiers was both proposed in [9-10]. This method has good imperceptibility and large embedding capacity, but suffers poor anti-detection capability because it will change the document characteristics. [11] also proposed to embed watermark by replacing or adding the these values and detect the watermark by utilizing the zero-knowledge proof. Mohamed Ahmed Mohamed *et al.* [12] suggested a method to hide information into a zero dimension image inserted into the document. Some more steganographic methods in OOXML format documents are summarized in [13], which are hiding information using OOXML relationship structure, using XML format feature, using XML format feature and OOXML relationship structure, and so on.

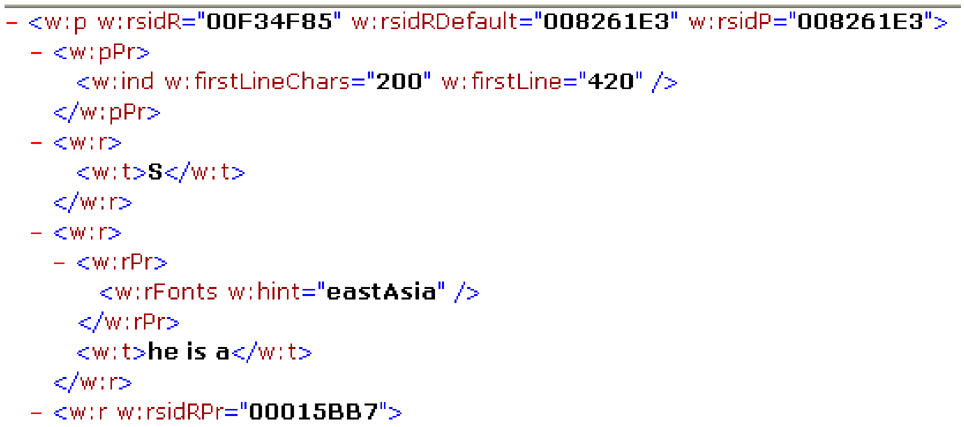
On the opposite, there is a technique called steganalysis, which detects the existence of the hidden information embedded in cover objects [14]. The steganalysis will break the security of the secret information. Therefore, steganographic methods should remain the cover-object unchanged or almost unchanged after the embedding process to resist the detection of steganalysis. Unfortunately, most of the existing steganographic methods for OOXML format documents did not pay much more attention to improve the anti-detection capability against steganalysis.

In order to improve the security of the steganography, this paper proposed to preserve the characteristics of the cover OOXML format document unchanged after embedding information into the values of the revision identifiers. Not only the replaced values of the revision identifiers in the main document body perform the same with the normal ones, but also the newly created values are added into other part to keep the internal data consistency during embedding information. Meanwhile, position marks are used to recognize the revision identifiers with the embedded information from the ones without information. Theoretical analysis and experiments demonstrate that the proposed method not only maintains the advantages of large embedding capacity, but also has good imperceptibility and anti-detection capability. The security of the method is higher than that of existing ones. It is a practical, effective and secure approach for covert communication and privacy protection.

2. Analysis of the Characteristics of the OOXML Format Document

2.1. Analysis of the Data Characteristics in the Main Document Body

As previously mentioned, Microsoft Word 2007 and later versions all adopt the OOXML format. An OOXML format file consists of a compressed ZIP package, and the package contains all parts of the document. In these parts, there is an essential part, which contains almost all the characters that should be shown on the MS Word display window and format properties of the word and the document that we can not easily see. Just referred to above is the main document body of the MS Word 2007 ZIP package, which is shown as document.xml. If you inspect the main document body, you will find that there are a set of special element attributes called revision identifiers(RI), which are almost ubiquitous in the main document body. The w: rsidR, w: rsidRPr, w: rsidRDefaul and w: rsidP defined by w:p elements and w: rsidRPr defined by w:r elements are all revision identifiers. Figure 1 shows the excerpt of the *document.xml* extracted from the ZIP package of a word 2007 document.



```
- <w:p w:rsidR="00F34F85" w:rsidRDefault="008261E3" w:rsidP="008261E3">
  - <w:pPr>
      <w:ind w:firstLineChars="200" w:firstLine="420" />
    </w:pPr>
  - <w:r>
      <w:t>S</w:t>
    </w:r>
  - <w:r>
    - <w:rPr>
        <w:rFonts w:hint="eastAsia" />
      </w:rPr>
      <w:t>he is a</w:t>
    </w:r>
  - <w:r w:rsidRPr="00015BB7">
```

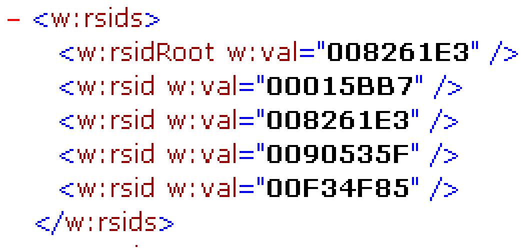
Figure 1. Excerpt of the Document.xml of an OOXML Format Document

Revision identifiers are mainly used to record the revisions of the document. As we all know, each electronic document may be revised several times by the author or somebody else before the final version. For an OOXML format document, the traces of these revisions (Here the revisions include the insertion, deletion and modification of the text or its format and so on) will be recorded by the revision identifiers. More precisely, they are recorded by the value of the revision identifiers. The value is composed of eight hex numbers. In other words, it is a 32-bit number stored in hexadecimal. It is worth noting that the value is randomly generated. It does not matter to the content of revision and the revision time or something else like that. That is to say, the value of a revision identifier has no specific meaning.

The observation of a large number of OOXML format documents found that although the value is randomly generated, there are some rules to follow. The former two hex numbers of the values are almost beginning with "00", and the next six hex numbers are actually generated randomly. At the same time, it was found that replacing the values of the revision identifiers don't affect the normal display and the use of the document. Based on this discovery, just the last three bytes(six hex numbers) of the values of the revision identifiers should be chosen to carry secret information in order to ensure the characteristics of the modified value accorded with the normal state. In this case, it is more difficult to detect the existence of secret information by the steganalysis, since the revision identifiers with or without information are the same.

2.2. Analysis of the Data Correlation Between Different Parts

By the analysis of revision identifiers in the main document body, the characteristics of the modified values can be kept accorded with the ones in the cover main document body. But the modifications would make effect to other parts in the cover document. As we all know, the ZIP package of an OOXML format document contains all parts of the document. Meanwhile, there are relationships between the parts. In these parts, there are two main parts include the revision identifiers: one is the main document body namely *document.xml*, the other is *settings.xml*. The w: rsid elements in the part *settings.xml* record all the values of the revision identifiers that have been created in the main document body, and each value is recorded only once. Figure 2 shows the excerpt of a settings.xml.



```
- <w:rsids>
    <w:rsidRoot w:val="008261E3" />
    <w:rsid w:val="00015BB7" />
    <w:rsid w:val="008261E3" />
    <w:rsid w:val="0090535F" />
    <w:rsid w:val="00F34F85" />
  </w:rsids>
```

Figure 2. Excerpt of a Settings.xml

Figure 1 and Figure 2 are obtained from the same Word 2007 document. Comparing the two figures, it shows the values of all revision identifiers generated in the main document body, are recorded in the values of <w: val> defined by the elements <w:rsid> in the part *settings.xml*. As we have seen in Figure 2, the values are arranged in ascending order by the hexadecimal value. Meanwhile, through the observation of a large number of word 2007 documents, it was found that if some revision identifiers in the main document body have a same value, the value is recorded only once. As shown in Figure 1, the attributes w: rsidRDefault and w: rsidP defined by the element <w:p>, their values both are "008261E3". But the part *settings.xml* as shown in Figure 2 contains only an element <w: rsid> with the value "008261E3".

Considering that there is a relation between the two parts, after modifying the values in the main document body, it is necessary to insert the same values in the part *settings.xml*. It is noteworthy that in the process of inserting, one should not duplicate record with the same values, and should finally ensure the values are still arranged in ascending order. In this way, it can not only maintain the consistency of the data within the main document body, but also conform with the internal data structure of OOXML format. As a result, it keeps the modified OOXML document innocuous, and improves the anti-detection capability and security.

2.3. A Characteristic-Preserving Steganographic Method

2.3.1. Position Mark

The revision identifier embedded information by replacing the last three bytes of its values is similar to others. In order to distinguish them, position mark should be designed to record the position of the embedded information. Here, the attribute “<w:rPr><w:rFonts w:hint="eastAsia"/></w:rPr>” in the main document body is defined as the Position Mark. This Position Mark will not be lost when the OOXML format document is operated with “Clear Format”, “Save as”, “Edit” and other operations. Moreover, the addition and deletion of a Position Mark doesn’t affect the normal display of the document. Therefore, if all the existing attribute <w:rFonts w:hint="eastAsia"/> are deleted, and then the Position Marks can be added to the paragraphs in which the revision identifiers are replaced to embed information. The use and appearance of the document will not be changed. And the secret information can be extracted according to the locations of the Position Marks.

2.3.2. Detailed Method

Based on the analysis of the OOXML format, a steganographic method is proposed in this paper, which is based on the revision identifiers. The w: rsidR, w: rsidRPr and w: rsidP defined by the element <w:p> are selected to hide secret information. The last six hex numbers of the values are successively replaced according to the hex numbers sequence converted from the secret information. Meanwhile, the Position Marks are added to the paragraphs where the revision identifiers are replaced. Then, the newly created values are added into the part *settings.xml*. To further enhance the security of the algorithm, symmetric encryption algorithm DES is used to encrypt the secret information. The method is described in detail as follows.

A. Embedding algorithm

Input: cover document D; secret message M; private key K .

Output: stego document D'.

Steps:

(1) Encrypt the secret message M by using DES algorithm and private key K to obtain encrypted message M'.

(2) Convert the encrypted message M' into hexadecimal sequence H.

(3) Read the content of the main document body *document.xml* from the decompressed ZIP archive of the cover document D.

(4) Locate a pair of paragraph element <w:p></w:p>, extract its attributes w:rsidR, w:rsidRPr and w:rsidP, and successively replace the last six hex numbers of their values with H. Meantime, record the newly created values of revision identifiers in set V.

(5) Extract the first run element <w:r></w:r> in this paragraph element, and insert the Position Mark <w:rPr><w:rFonts w:hint="eastAsia"/></w:rPr> into it.

(6) Go to the next pair of paragraph element, repeat step 4 - 5 until the entire hexadecimal sequence H has been embedded.

(7) Read content of the part *settings.xml* from the compressed ZIP archive of the cover document D. Extract the pair of element <w: rsids></w: rsids>, and insert all the elements of V into it as its child element <w: rsid>, while ensuring that its child elements do not contain duplicate values.

(8) Compress all the parts as a ZIP archive and rename it to a stego document D'.

It is worthwhile to note that the cover document would be preprocessed to contain no attribute <w:rFonts w:hint="eastAsia"/> before embedding information.

B. Extraction algorithm

Input: stego document D'; private key K.

Output: secret message M .

Steps:

(1) Decompress the ZIP archive of the stego document D', and read content of the main document body *document.xml*.

(2) Locate each paragraph element <w:p> which contains the Position Mark, then extract its attributes w:rsidR,w:rsidRPr and w:rsidP, and successively add the last six hex number of their values to a hexadecimal sequence H.

(3) Repeat step 2 until all the paragraph elements have been browsed.

(4) Convert H to a character string M'.

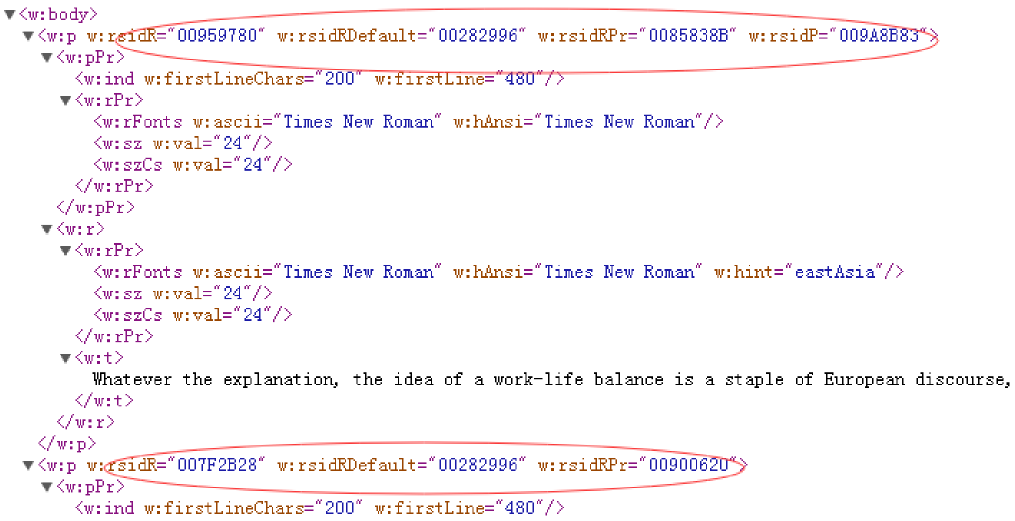
(5) Decrypt M' by using DES algorithm with private key K to obtain the secret message M .

3. Experimental Results and Analysis

3.1. Imperceptibility

The secret information is embedded by replacing the values of the revision identifiers in the main document body. The changes of the values will neither be shown on the MS Word display window, nor affect the use of the document. That is to say, the proposed method neither changes the content of the text, nor changes the format of the characteristics. There is no visual difference between the original cover document and the corresponding stego one.

At the same time, the proposed method keeps the characteristics of the modified values of the revision identifiers accorded with the normal states. This makes it more difficult to distinguish the values carrying secret message from the normal values by steganalysis or human vision systems. Figure 3 shows subsection of the main document part *document.xml* of an example stego Word2007 document, whose revision identifiers have been embedded secret information by the proposed method. As can be seen from the figure, the revision identifiers with secret information look the same as the ones without being changed, because their values are still in line with normal characteristics. Compared with similar steganographic algorithm, the method proposed in this paper has better imperceptibility. For example, the algorithms described in [9] replaced the values of the revision identifiers completely. The generated stego documents contained abnormal values of revision identifiers, whose first two hex numbers were always nonzero. It is so obvious that the stego document can easily lead to the suspicion of the third party.



```
▼<w:body>
  ▼<w:p w:rsidR="00959780" w:rsidRDefault="00282996" w:rsidRPr="0085838B" w:rsidP="009A8B83">
    ▼<w:pPr>
       <w:ind w:firstLineChars="200" w:firstLine="480"/>
      ▼<w:rPr>
         <w:rFonts w:ascii="Times New Roman" w:hAnsi="Times New Roman"/>
         <w:sz w:val="24"/>
         <w:szCs w:val="24"/>
       </w:rPr>
     </w:pPr>
    ▼<w:r>
      ▼<w:rPr>
         <w:rFonts w:ascii="Times New Roman" w:hAnsi="Times New Roman" w:hint="eastAsia"/>
         <w:sz w:val="24"/>
         <w:szCs w:val="24"/>
       </w:rPr>
      ▼<w:t>
         Whatever the explanation, the idea of a work-life balance is a staple of European discourse,
       </w:t>
     </w:r>
   </w:p>
  ▼<w:p w:rsidR="007F2B28" w:rsidRDefault="00282996" w:rsidRPr="00900620">
    ▼<w:pPr>
       <w:ind w:firstLineChars="200" w:firstLine="480"/>
```

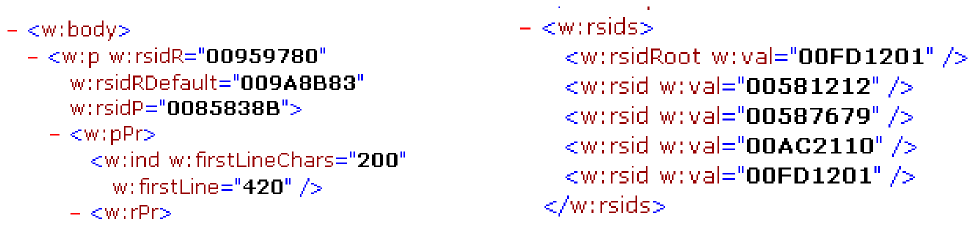
Figure 3. Excerpt of Document.xml of an Example Word 2007 Document with Hidden Information

3.2. Anti-Detection Capability

The proposed method not only guarantees the characteristics of the modified values accorded with the normal state, but also keeps the internal data consistency of the cover and stego document by inserting all the created values to the part *settings.xml*. It normalizes the stego documents as much as possible to improve the anti-detection and anti-forensics capability when suffering from steganalysis and forensics attacks[14].

Figure 4 shows the subsection of the main document part *document.xml* and the part *settings.xml* from an example stego document generated by the method in [10]. The last six hex numbers of the values of the attributes w:rsidR, w:rsdRDefault, w:rsidP in *document.xml* are replaced to embedding information. It is obvious that some values of revision identifiers in *document.xml* are not existent in the part *settings.xml*. Taking the same cover document and secret information to conduct experiment, the subsections of those two parts generated by the proposed method are shown in Figure 5. Three different revision identifiers w:rsidR, w:rsdRPr, w:rsidP are chosen to be replaced or added to embedding information. As the embedded information is the same as that embedded by the method in [10], thus the values of these three revision identifiers are the same as those three revision identifiers w:rsidR, w:rsdRDefault, w:rsidP in Figure 4. It can be clearly seen that the newly created values synchronously appear in the part *settings.xml*. The updated *settings.xml* also maintain the same organizational structure by inserting the new values into the pair of element <w: rsids> </ w: rsids> as its children in increasing order. This results that the *settings.xml* in a stego document has the same characteristics with that in the normal one.

To compare the anti-detection capability of the proposed method with the one proposed in [10], a steganalysis scheme is designed to detect the generated stego documents. Its core idea is described as follows: Compare the values of the revision identifiers from the two parts namely the main document body *document.xml* and the part *settings.xml*. If the values in the *document.xml* are all present in the part *settings.xml*, then the document is identified as a normal document. On the contrary, as long as there is a value does not exist in the part *settings.xml*, the document is directly identified as a stego document.

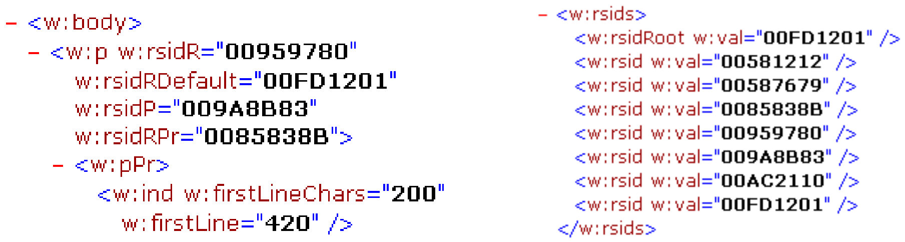


```
- <w:body>
  - <w:p w:rsidR="00959780"
      w:rsidRDefault="009A8B83"
      w:rsidP="0085838B">
    - <w:pPr>
        <w:ind w:firstLineChars="200"
          w:firstLine="420" />
      - <w:rPr>
```

```
- <w:rsids>
    <w:rsidRoot w:val="00FD1201" />
    <w:rsid w:val="00581212" />
    <w:rsid w:val="00587679" />
    <w:rsid w:val="00AC2110" />
    <w:rsid w:val="00FD1201" />
  </w:rsids>
```

(a) Excerpt of Document.xml (b) Excerpt of Settings.xml

Figure 4. The Parts of an Example Stego Document Generated By [10]



```
- <w:body>
  - <w:p w:rsidR="00959780"
      w:rsidRDefault="00FD1201"
      w:rsidP="009A8B83"
      w:rsidRPr="0085838B">
    - <w:pPr>
        <w:ind w:firstLineChars="200"
          w:firstLine="420" />
```

```
- <w:rsids>
    <w:rsidRoot w:val="00FD1201" />
    <w:rsid w:val="00581212" />
    <w:rsid w:val="00587679" />
    <w:rsid w:val="0085838B" />
    <w:rsid w:val="00959780" />
    <w:rsid w:val="009A8B83" />
    <w:rsid w:val="00AC2110" />
    <w:rsid w:val="00FD1201" />
  </w:rsids>
```

(a) Excerpt of Document.xml (b) Excerpt of Settings.xml

Figure 5. The Parts of an Example Stego Document Generated by the Proposed Method

After applying the stegonagraphy method based on revision identifiers in [10] and that in this paper to 308 Word 2007 documents which were randomly downloaded from the Internet, we feed the two resulting groups of stego documents and the original ones into the above designed steganalysis system, with 308 documents in each group as mentioned before. Table 1 shows the detection result. As seen from the table, the false negative rate of the method in [10] is 0, which means that it is completely incapable of resisting the inspection from the steganalysis designed in this paper, while that of our method is 96.8%. Nearly all the stego documents of our method cannot be recognized accurately. Therefore, it is obvious that our method possesses the better anti-detection capability than that of the method in [10]. Note that a few documents in the original group are also detected as stego ones, which is caused by the fact that some revision identifiers in the main document body of these documents do not exist in the corresponding *settings.xml*. From the false positive rate list in the Table 1, we can see they occupy approximately 3.6%, which gives a sound reason why the method in our paper cannot achieve 100% false negative rate.

Table 1. Steganalysis Results

Document Set	Documents	Stego Documents	False Negative Rate	False Positive Rate
Stego Document based on [10]	308	308	0%	—
Stego Document based on Our Method	308	10	96.8%	—
Normal Document	308	11	—	3.6%

3.3 Embedding Capacity

The method proposed in this paper replaces the last six hex numbers of the attribute values of revision identifiers to embed the secret information. Therefore, replacing or inserting a revision identifier can hide 24 bits information, which equal to the long of six hex numbers. Namely, 72 bits information can be embedded into each <w:p> element as we have chosen three revision identifiers w: rsidR, w: rsidRPr, w: rsidP of the alternative revision identifiers in each <w:p> element. Suppose a document has N <w: p> elements, then the embedding capacity C of the document is:

$$C = 3 * 24 * N \quad \text{(bits)} \tag{1}$$

From Equation 1, it can be seen that the embedding capacity C is positively correlated with N. C will be increased with the increasing N. Namely, the document has more paragraphs(<w:p> elements), the number of revision identifiers being available to embed information is larger, the embedding capacity of the proposed method is larger. Compared to the existing natural language text steganography methods, the proposed method has a satisfying embedding capacity.

3.4. Security Analysis

Through above experiments and analysis, we can see that the proposed method has a good imperceptibility and anti-detection capability. It is unlikely to cause illegal attacker's attention and suspicion by using this method to transmit secret information. The risk of revealing the secret information is reduced, while raising security of the secret information. In addition, as we all know the security of a steganographic scheme not only depend on the scheme being kept secret. So, an encryption algorithm DES is used to encrypt the secret information before it is embedded into the document. Even though a third party is aware of the existence of secret information, retrieving the secret information accurately is such a difficult thing unless they know the private key. Thus, the proposed method has achieved a higher level of security.

4. Conclusion

A steganographic method for the OOXML format document is proposed in this paper. Secret information is embedded by replacing the values of the revision identifiers in the main document body. Meanwhile, the newly created values are added into the related part. The experimental results have shown that the proposed method achieved good imperceptibility and anti-detection capability resulting in high security, and provided large embedding capacity. It is a practical, effective and secure approach for covert communication and privacy protection. There are mainly two things to do next. One is to improve its robustness so that it can resist "Insert", "Delete" and other potentially document edit operations. The other is to develop a watermarking scheme based on the proposed method to detect and locate the tamper in the document.

Acknowledgements

This project is supported by National Natural Science Foundation of China (Nos. 61202439, 61202496, 61303042), Hunan Provincial Natural Science Foundation of China (Grant No.13JJ2031).

References

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, “Information Hiding-A Survey”, Proceedings of the IEEE, vol. 87, no. 7, **(1999)**, pp. 1062-1078.

[2] A. Cheddad, J. Condell, K. Curran and P. McKevitt, “Digital Image Steganography: Survey and Analysis of Current Methods’, Signal Processing **(2010)**, vol. 90, pp. 727-752.

[3] [3] P. C. Su, M. T. Lu, C. Y. Wu. ‘A Practical Design of High-Volume Steganography in Digital Video Files”, Multimedia Tools and Applications, vol. 66, no. 2, **(2013)**, pp. 247-266.

[4] S. Ahani, S. Ghaemmaghami and Z. Wang, “A Sparse Representation-Based Wavelet Domain Speech Steganography Method”, IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 23, no. 1, **(2014)**, pp. 80-91.

[5] “ECMA International. Office Open XML File Formats”, Part 1. ECMA-376. 1st ed., **(2006)**, pp. 11.

[6] B. Park, J. Park and S. Lee, “Data Concealment and Detection in Microsoft Office 2007 Files”, Digital Investigation, vol. 5, no. 3, **(2009)**, pp. 104-114.

[7] Z. J. Fu, X. M. Sun, Y. L. Liu and B. Li, “Text Split-based Steganography in OOXML Format Documents for Covert Communication”, Security and Communication, vol. 5, no. 9, **(2012)**, pp. 957-968.

[8] S. L. Garfinkel and J. Migletz, “New XML-based Files Implications for Forensics”, IEEE Security and Privacy, vol. 7, no. 2, **(2009)**, pp. 38-44.

[9] M. Xu, Y. Wang and T. Li, “A Novel Scheme of Information Hiding in Word 2007 Document”, Journal of Computer Research and Development (in Chinese), vol. 4, no. 6, **(2009)**, pp. 112-116.

[10] A. Castiglione, “Hiding Information into OOXML Documents: New Steganographic Perspectives”, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 2, no. 4, **(2011)**, pp. 59-83.

[11] Z. Fu, X. Sun, J. Zhang and B. Li, “A Novel Watermark Embedding and Detection Scheme Based on Zero-Knowledge Proof”, Journal of Digital Content Technology and its Applications, vol. 5, no. 3, **(2011)**, pp. 273-286.

[12] M. A. Mohamed, G. A. Obay, M. O. Ismail and M. O. Elobied, “A Novel Method to Protect Content of Microsoft Word Document Using Cryptography and Steganography”, International Journal of Computer Theory and Engineering, vol. 7, no. 4, **(2015)**, pp. 292-296.

[13] M. A. Raffay, “Data Hiding and Detection in Office Open XML Documents”, University of Ontario Institute of Technology, Oshawa, Ontario, Canada, **(2011)**.

[14] A. Nissar and A. Mir, “Classification of Steganalysis Techniques: A Study”, Digital Signal Process, vol. 20, no. 6, **(2010)**, pp. 1758-1770.

[15] Z. J. Fu, X. M. Sun, Y. L. Liu and B. Li, “Forensic investigation of OOXML format documents”, Digital investigation, vol. 8, no. 1, **(2011)**, pp. 48-55.

Authors

Lingyun Xiang, she received her BE degree in computer science and technology, in 2005, and the PhD degree in computer application, in 2011, Hunan University, Hunan, China. Currently, she is a Lecturer in School of Computer and Communication Engineering, Changsha University of Science and Technology, Hunan, China. Her research interests include network and information security, steganography, steganalysis, machine learning.

Caixia Sun, she received her BE degree in networking engineering, in 2013, and the MS degree in computer technology, in 2015, Changsha University of Science and Technology, Hunan, China. Her research interests include information security and steganography.

Niandong Liao, he was received his BE degree from Shanxi University in 2001, MS degree in computer application from Guizhou University in 2006, and PhD degree in information security from Beijing Jiaotong University in 2009, respectively. Currently, he is a Lecturer in School of Computer and Communication Engineering, Changsha University of Science and Technology, Hunan, China. His research interests include network and information security, artificial intelligence.

Weizheng Wang, he was received his BS degree in applied mathematics from Hunan University in 2005 and the PhD degree in technology of computer application from Hunan University in 2011, respectively. Currently, he is a Lecturer in School of Computer and Communication Engineering, Changsha University of Science and Technology, Hunan, China. His research interests include built-in self-test, design for testability, low-power testing, and test generation.