http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 11 (8): 1084-1090, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.1084.1090
© 2012 Asian Network for Scientific Information

A Novel Reversible Text Data Hiding Scheme

[1]Bin Yang, [2]Xingming Sun, [3]Jianjun Zhang, [3]Lingyun Xiang, [3]Xianyi Chen and [3]Xu Li
[1]Department of Information Engineering and Technology, NanHai Campus,
South China Normal University, Foshan, 528200, China
[2]Jiangsu Engineering Center of Network Monitoring,
Nanjing University of Information Science and Technology, Nanjing, 210044, China
[3]School of Information Science and Engineering, Hunan University, Changsha, 410082, China

Abstract: In many critical application areas, such as military, legal and literature fields, methods of protecting copyright for text data could not cause any distortion in textual content. In this study, we evaluate a novel reversible (lossless) data hiding scheme for MS office 2007 document. The proposed scheme modifies the unnoticeable content and the synonyms of a document to hide information. While in extraction processing, the original content can be recovered without any distortion from the marked textual. Our scheme is achieved by using two common text information hiding methods simultaneously. The secret information is embedded into the cover document by synonym substitution. Original synonyms in the document are mapped into a compressed Synonym Index Table (SIT) and concealed into the MS office 2007 document. Experiments results demonstrated that proposed scheme can not only successfully embed and extract the secret information but also keep the original textual content undistorted.

Key words: Data hiding, reversible, synonym substitution, synonym index table, MS office 2007 documents

INTRODUCTION

Data hiding is the technique that inserts data into the cover multimedia imperceptibly. In the last decade, data hiding technique have been explored extensively for multimedia files (Topkara *et al*., 2006; Chen *et al*., 2010; Zeng and Wu, 2010; Chandra and Khan, 2010; Liang *et al*., 2011; Li *et al*., 2011). In spite of that, document is one of the most prevalent and indispensable form of information nowadays and always be used as a cover medium (Yang *et al*., 2011; Borges *et al*., 2008). The text data hiding scheme mainly includes three types: schemes using characteristics of the text (Brassil *et al*., 1999; Rabah, 2004), schemes using the structure of files (Cantrell and Dampier, 2004; Castiglione *et al*., 2007) and schemes using natural language processing (Topkara *et al*., 2005; Wang *et al*., 2008). The last one called natural language data hiding has great security and robustness and it has become the most commonly used scheme for text data hiding.

Most multimedia data hiding techniques modify and hence distort the host data in order to insert the additional information. Often, this embedding distortion is small but still irreversible, i.e., it cannot be removed to recover the cover host data. An intriguing feature of reversible data embedding is reversibility, that is, one can remove the embedded data to restore the cover data.

In some applications, such as medical diagnosis and law enforcement, it is critical to archiving of valuable original works after the hidden data are extracted for some legal consideration (Ni *et al*., 2006). Any changes of the content will affect the access to the real meaning of the document. Although some insertion distortion is admissible in some circumstance, permanent loss of content fidelity is undesirable. This highlights the requirement for reversible data hiding techniques.

Recently, a number of reversible data hiding schemes have been proposed by using techniques, such as circular interpretation of the bijective transform (De Vleeschouwer *et al*., 2003), lowest levels replacement (Celik *et al*., 2005), difference expansion (Tian, 2003), recovery visible package (Yang *et al*., 2009; Hong *et al*., 2009), histogram shifting (Hong *et al*., 2010) or Prediction-Based (Coltuc, 2011). Nevertheless, these schemes are applicable only to images, few reversible data hiding scheme have studied on embedding data in text document. Liu *et al*. (2010) proposed a reversible text watermarking scheme by using an invertible transform to perform the embedding and extracting process. However, due to the low embedding rate and the strict requirements

Corresponding Author: Xingming Sun, Jiangsu Engineering Center of Network Monitoring,
Nanjing University of Information Science and Technology, Nanjing, 210044, China

on the cover text, Liu's scheme is hard to put into practical application.

Microsoft (MS) office system 2007 since its launch, due to the advantage of its file format, has been accepted by more and more users. Park *et al.* (2009) proposed a method to embed secret information in MS office 2007 document by creating unnoticeable contents which can be created by using the concept of ''content relationship''.

In this study, we proposed a novel scheme that uses a combination of two common methods to achieve reversible data hiding. Cover text file is compressed and inserted in the MS office 2007 document as an unnoticeable content. Then, the secret information is embedded into the cover text by synonym substitution. The proposed technique could be applied not only to MS office document but also to other structure base documents, such as PDF etc., Moreover, the security, robustness and capacity of the proposed scheme are also discussed.

RELATED WORK

Our proposed scheme on reversible text data hiding uses a combination of two common data hiding methods: the synonym substitution approach and the MS office 2007 documents structural approach.

The synonym substitution approach: In order to embed data in natural language text unnoticeably, a systematic method for modifying, or transforming text should preserve the grammaticality of the sentences. Synonym substitution is the most widely used linguistic transformation for information hiding systems since it is a relatively straightforward linguistic data hiding method (Topkara *et al.*, 2005).

Early in 1996, Bender *et al.* (1996) described the method based on synonym substitution roughly. First they defined a synonym table by a synonym dictionary such as WordNet. For example, '0' was represented to the word 'big', '1' to 'large' and then the encoder replaced the selected words by their synonyms in the text.

A simplified example of synonym substitution is given in Fig. 1. The secret bit string '011' is to be embedded which can be divided into two code words '01' and '1' and the information carriers in the cover text are the words like and big. According to the encoding dictionary, enjoy represents '11' and beautiful represents '0', then these words are chosen to replace the original words in the cover sentence. The embedded sentence "I love this large house" finally is sent to the receiver. The receiver only needs an encoding dictionary and the decoding algorithm to extract the secret message.

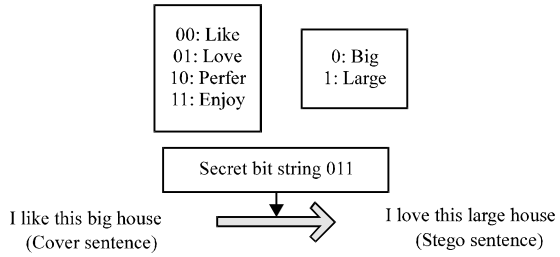

Fig. 1: An example of synonym substitution

Most of synonym substitution methods are more or less modified the real meaning of the original text and this is not tolerated in some applications, i.e. reversible data hiding technique is needed.

The MS office 2007 documents structural approach: MS office documents (e.g., Word, PowerPoint and Excel) are most widely used document types at present. In recent years, several methods for hiding data in MS office documents have been proposed (Cantrell and Dampier, 2004; Castiglione *et al.*, 2007). However, these methods are mainly aimed at the MS office 1997-2003 documents and not specifically for new MS office 2007 documents. Park *et al.* (2009) demonstrated that how data concealment in MS office 2007 documents is possible. They used OOXML files to define customized parts, relationships, or both within a MS office 2007 document to store and conceal information.

It is well known that MS office 1997-2003 documents are binary files but MS office 2007 documents use a new file format based on OOXML format (Fu *et al.*, 2011). The MS office 2007 documents are consisted of many compressed component parts that store in a ZIP format package and each decompressed package conforms to the OOXML file format. A package is an ordinary Zip file which contains package content-type item, relationship items and parts (ECMA International, 2006). An OOXML file is based on the following:

- Package: ZIP archive
- Part: Files in ZIP archive
- Relationship: The relationships between the parts and package or among parts

There are many unknown parts and unknown relationships in OOXML file which will not affect the appearance and content of the OOXML file. It is possible to hide secret files by creating several unknown parts and its corresponding relationships. First, the encoder copies the secret files to the carrier archive file directory. Then, the encoder insert codes which define the secret files

```
a<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Types xmlns="…">
<Default Extension="rels" ContentType="…"/>
<Default Extension="xml" ContentType="application/xml"/>
<Default Extension="zip" ContentType="application/zip"/><Override
PartName="/word/document.xml" ContentType="…"/>
…
</Types>a
```

Fig. 2: [Content_Types].xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< Relationships xmlns="…">
<Relationship Id="rId3" Type="…" Target="docProps/app.xml"/>
<Relationship Id="rId2" Type="…" Target="docProps/core.xml"/>
<Relationship Id="rId1" Type="…" Target="word/document.xml"/>
<Relationship Id="rId101" Type="http://schemas. openxmlformats.
org/officeDocument/2006/relationships/a" Target="s.zip"/>
</Relationships>
```

Fig. 3: Relationship file

extensions and its associate paths into the "[Content_Types].xml". Finally, the encoder modifies the relationship file, changes the secret information files type and its IDs. After "[Content_Types].xml" was modified the secret files became unknown parts of the document. For example, a secret file "s.zip" is to embed into the cover document (in this example, an MS Word 2007 file). The encoder add a string (in bold and italic) into "[Content_Types].xml" and relationship file which are shown in Fig. 2, 3.

A MS office 2007 document containing these hidden files can be opened normally. Thus these secret files are hidden completely without causing notification and cannot be detected by any of the functions supported by MS office 2007 applications (Park *et al*., 2009).

THE PROPOSED SCHEME

Here, a reversible text data hiding scheme is presented. The proposed data hiding scheme described below composes of the embedding and extraction process.

As stated earlier, the reversible text data hiding refers to natural language data hiding. And the most popular natural language data hiding scheme is based on synonym substitution. However, the method was irreversible i.e., the cover text was permanently transformed into a modified text when some synonyms were substituted. This shortcoming could be remedied by embedding the cover text information into the structure of MS office documents.

The basic idea of the proposed scheme is to use two common embedding methods to embed the cover text T and the secret information M into a cover document D, respectively. As shown in Fig. 4, cover document D consisted of the text T and many compressed component parts S. In data embedding process, cover text T was inserted into the component parts S as an unknown content firstly, then the cover text T was replaced to a stego text T' by synonym substitutions.

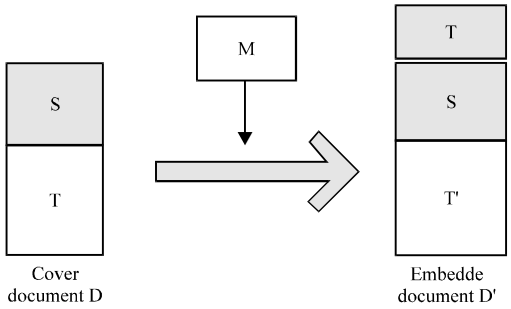

Fig. 4: Data embedding process

(a)

When the sexes differ in beauty in the power of singing, or in producing what i have called instrumental music, it is almost invariably the male who surpasses the female. These qualities, as we have juet seen, are patently of high importance to the male. When they are gained for only a part of the year it is always before the breeding season. It is the male alone who intricately display with varied attractions and often performs strange antics on the ground or in the air, the presence of the female. Each male drives away, or if he can, kills his rivals. Hence we may conclude that it is the object of the male to induce the female to pair with him and for this purpose he tries to excite or charm her in various ways and this is the opinion of all those who.

(b)

```
00010000010010000000100000000000011001001000100000100000
00000001001000001000000000000001001000000100000000000000
00001010000100001000000000000000010000000000000000010
00001000011010100100000010110000000100 0
```

Fig. 5(a-b): (a) A cover text and (b) Its corresponding SIT

The synonym index Table (SIT) generation: The original words that would be modified in the embedding process should be saved into the component parts of document. And all the modified words were synonyms, thus, the proposed scheme generated a SIT firstly. SIT consisted of the original words' synonym index in the dictionary. For a word W having synonyms in the dictionary, we got its index number t in its synonym set and then, saved the index number t into the SIT in binary format. To illustrate, an example of cover textual content and its corresponding SIT is provided in Fig. 5.

Reversible data embedding process: As described above, the original words were saved into a SIT. However, it is not all the words which have synonyms would be

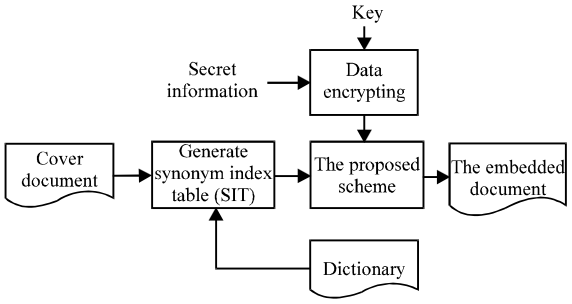

Fig. 6: The embedding process

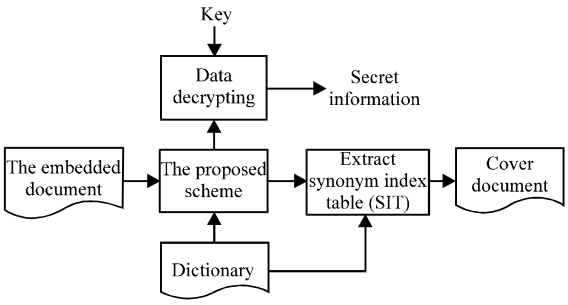

Fig. 7: The extracting process

substituted when the secret information was embedded. For the sake of imperceptibility, the SIT just saves the synonym index numbers of synonyms which are about to be substituted. Therefore, the substitution sets of the words which will be substituted should be found out before generating the SIT. Figure 6 depicts the embedding process of the proposed scheme and it consists of following steps:

- **Step 1:** Encrypt the secret information by any of various encryption algorithms such as RC2, RC4, DES, etc.
- **Step 2:** Pre-embed the encrypted secret information by the synonym substitution-based embedding method. Then, the substitution sets of the words which were substituted by their synonyms were obtained
- **Step 3:** Judge whether there is enough space for embedding the secret information, if enough, then proceed to the next step, otherwise warn the user of insufficient embedding capacity
- **Step 4:** Generate the Synonym Index Table (SIT) which consisted of the original words' synonym index in the dictionary. The substitution sets of the words were obtained in step 2
- **Step 5:** Embed the file containing the SIT into the MS Office document
- **Step 6:** Embed the encrypted secret information by the synonym substitution method and outputs the embedded document

In step 4, the SIT File Extension is often modified into more common ones, such as jpg, gif. In step 5, the encoder should decompress the MS Office document first and modify the "[Content_Types].xml" file and relationship file to make the SIT file into an unknown part of the document. Finally, the encoder compresses all parts of the MS Office document to form an embedded document containing the SIT file.

Secret information extraction and the cover textual content retrieving process: The proposed extraction has two purposes. One is extracting the secret information from and the other is restoring the cover text process the embedded document. Figure 7 depicts the extracting process of the proposed scheme mainly including four steps:

- **Step 1:** Unzip the MS office document and get the SIT file from the component parts of the document
- **Step 2:** Extract the encrypted secret information by the synonym substitution-based method and recover the embedded textual content to the original text
- **Step 3:** Decrypt the secret information which was encrypted by the encryption key
- **Step 4:** Out put the cover document and the secret information

In step 2, we have made some modifications to the synonym substitution-based method. First, for a word *W'* having synonyms in a dictionary, the decoder find its original index t in the SIT. Second, the decoder extract the embedded information while reversed W' to the original word W.

EXPERIMENTAL RESULTS AND DISCUSSION

The proposed scheme was implemented by Visual C++6.0 and used the trash space of MS office Word 2007 document to save the cover text and run on the Pentium Dual, 2.2 GHz CPU and 1 GB RAM hardware platform. Since the synonym substitution method was used to embed the secret information, a dictionary was needed. The most widely known such dictionary is WordNet (Fellbaum, 1998). In WordNet English nouns, verbs, adjectives and adverbs are organized into synonym sets and each set represents an underlying lexical concept. The content of WordNet 2.0 is summarized in Table 1 (Jurafsky and Martin, 2000). In this scheme, WordNet 2.0 lexical database was utilized to obtain sets of synonymy for the substitution purpose.

In experiments, a short novel saved as MS office Word 2007 format was used as a cover document which was shown in Fig. 5a. Assuming the secret information to be embedded is "YB2011", RC4 was used to encrypt the secret information.

Table 1: WordNet 2.0 database statistics

Category	Unique strings	No. of senses
Noun	114648	141690
Verb	11306	24632
Adjective	21436	31015
Adverb	4669	5808
Total	152059	203145

After the step 1 and step 2 which mentioned in embedding process, the substitution sets of the words which will be substituted were obtained. To shorten the length coding and enhance the coding efficiency, Huffman code was used to encode the substitution sets. As an example, for a word "humans", its synonyms "mankind" and "humankind" and their Huffman code were "0", "01"and "10". The encoder created the corresponding SIT as can be seen from Fig. 5b and embedded it into the document's trash space.

As the cover text was accurate preserved, secret information can be embedded into the text by synonym substitution.

Figure 8 shows the stego text generated by our proposed scheme and the cover text is shown in Fig. 5a. The words which are underlined were substituted in the embedding process.

Security, robustness and capacity: There are three different aspects in information-hiding scheme contend with each other: capacity, security and robustness (Provos and Honeyman, 2003). The cover text was replaced by synonym substitution, replacing a word by a word with similar meaning, this may make the text which is anomalous at the document level, or anomalous with regard to the state of the world in the proposed scheme (Chang and Clark, 2010). The marked MS office document which is produced by using the proposed method will not be shown on the screen display. Moreover, the embedded document can resist "Format", "Impersonation", "Save As", "Copy" and other active attacks (Fu *et al*., 2011). Hence, the proposed scheme by using a combination of above two methods has a good security and robustness.

Capacity, as one of the most important aspect in data hiding, regards to the number of secret information bits could be hidden in the cover medium (Yang *et al*., 2011). In this paper, we discuss two aspects. First, we consider the capacity of data hiding in the MS office 2007 document. In MS office 2007 document, a file can be compressed and concealed into the package by using unknown parts and unknown relationships (Park *et al*., 2009). The hidden file size is not restricted, so the size of SIT file theoretically is unlimited. Furthermore, the SIT file which had been compressed reversible generally is very small, so it is hard to be detected when it was concealed into MS office 2007 document. Second, we consider the capacity of data hiding in cover text by synonym substitution method. The capacity has great direct relationship to the cover text size and the synonym substitution strategy, the longer of cover text, the higher of capacity. Therefore, we only consider the embedding bit rate in different substitution strategy. In this study, two strategies were compared, one is strict and the other is relative loose. For simplicity, we name them as strategy1 and 2, respectively.

The only mathematically formal type of linguistic synonymy is when the compared words can replace each other in any context without any change in meaning. These are absolute synonyms, e.g., agleam and nitid (Bolshakov and Gelbukh, 2004; Liu *et al*., 2008). Otherwise, the words that may change the meaning while replacing, we name them non-absolute synonyms. In strategy1, the strict one, a word can only be replaced when it is absolute synonym. A word can be replaced while it is non-absolute synonym in strategy 2.

A set of experiments are conducted to measure the data embedding bit rate of the proposed method when using the above two strategies. Ten theses, five journal papers and five newspapers were selected as the experiments cover text. Figure 9 depicted the embedding bit rate in different strategies. The embedding bit rate

When the sexes differ in beauty in the power of singing, or in producing what i have called instrumental music, it is almost invariby the male who surpasses the female. These qualities, as we have juet seen, are evidently of high importance to the male. When they are gained for only a part of the year it is always before the breeding season/ It is the male alone who elaborately display with varied attractions and often perfomes strage antics on the ground or in the air, the presence of the female. Each male drives away, or if he can, kills his rivals. Hence we may conclude that it is the object og the male to induce the female to pair with him and for this purpose he tris to axcite or charm her in various ways and tis the opinion of all those who

Fig. 8: A stego text generated by our proposed scheme

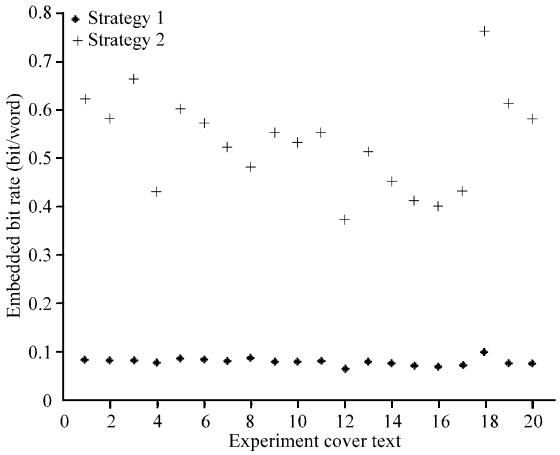

Fig. 9: Embedding bit rate in different strategies

in strategy 2 is higher than that in strategy 1 because more words had been substituted. However, the higher embedding bit rate always leads to the poorer imperceptibility. In the proposed scheme, strategy 1 is used to get the best imperceptibility and only when the capacity is not enough, strategy 2 is selected.

CONCLUSION

One common drawback of virtually all data hiding methods is the fact that the cover text is inevitably distorted by some embedding process. Although this distortion is often quite small, it may not be accepted in military, legal, etc., In this study, a novel scheme is developed for reversible data hiding. It enables the exact recovery of the cover text upon extraction of the embedded information. The scheme is achieved by simultaneously using two common methods of information hiding. Cover text is transformed into the compressed SIT file and is embedded as an unknown part with unknown relationship in OOXML file. Then secret information is embedded into the cover document by the synonym substitution.

At this stage, the authors just realized using the combination of synonym substitution and file structure methods. More experiments would be done due to the rapid improvements in natural language data hiding techniques in the future. And a combination of other different methods may be used to achieve higher performance.

ACKNOWLEDGMENTS

This study is supported by the National Natural Science Foundation of China (60736016, 60973128, 61173142, 61103215, 61070196, 61173141, 61172156 and 61173136), National Basic Research Program 973 (2010CB334706 and 2011CB311808), PAPD fund, the 3rd Guangdong Province 211 program for key subject development. Scientific Research Fund of Xiangtan University (No. 11QDZ41). Human Provincial Education Department (No. 11C1215). Human Science and Technology Department (No. 2011GK3205).

REFERENCES

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Bolshakov, I.A. and A. Gelbukh, 2004. Synonymous paraphrasing using WordNet and internet. Proceedings of the 9th International Conference on Applications of Natural Language to Information Systems, June 23-25, 2004, Salford, UK., pp: 189-200.

Borges, P., J. Mayer and E. Izquierdo, 2008. Robust and transparent color modulation for text data hiding. IEEE Tran. Multimedia, 10: 1479-1489.

Brassil, J.T., S. Low and N.F. Maxemchuk, 1999. Copyright protection for the electronic distribution of text documents. Proc. IEEE, 87: 1181-1196.

Cantrell, G. and D.D. Dampier, 2004. Experiments in hiding data inside the file structure of common office documents: A steganography application. Proceedings of the International Symposium on Information and Communication Technologies, June 16-18, 2004, Las Vegas, Nevada, USA., pp: 146-151.

Castiglione, A., A.D. Santis and C. Soriente, 2007. Taking advantages of a disadvantage: Digital forensics and steganography using document metadata. J. Syst. Software, 80: 750-764.

Celik, M.U., G. Sharma, A.M. Tekalp and E. Saber, 2005. Lossless generalized-LSB data embedding. IEEE Trans. Image Process., 14: 253-266.

Chandra, S. and R.A. Khan, 2010. Object oriented software security estimation life cycle-design phase perspective. J. Software Eng., 4: 185-192.

Chang, C.Y. and S. Clark, 2010. Linguistic steganography using automatically generated paraphrases. Proceedings of the Human Language Technologies: Conference of the North American Chapter of the Association of Computational Linguistics, June 2-4, 2010, Association for Computational Linguistics, Los Angeles, California, USA., pp: 591-599.

Chen, H., H. Luo, F.X. Yu, Z.L. Huang and J.X. Liu, 2010. Progressive satellite image transmission based on integer discrete cosine transform. Inform. Technol. J., 9: 169-173.

Coltuc, D., 2011. Improved embedding for prediction-based reversible watermarking. IEEE Trans. Inform. Forensics Secur., 6: 873-882.

De Vleeschouwer, C., J.F. Delaigle and B. Macq, 2003. Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Trans. Multimedia, 5: 97-105.

ECMA International, 2006. Office open XML file formats. http://www.ecma-international. org/ publications/ standards/Ecma-376.htm

Fellbaum, C., 1998. WordNet: An Electronic Lexical Database. 1st Edn., MIT, Press Cambridge, MA., USA., ISBN-10: 026206197X, pp: 423.

Fu, Z., X. Sun, J. Zhang and B. Li, 2011. A novel watermark embedding and detection scheme based on zero-knowledge proof. Int. J. Digital Content Technol. Appl., 5: 273-286.

Hong, W., J. Chen and T.S. Chen, 2009. Blockwise reversible data hiding by contrast mapping. Inform. Technol. J., 8: 1287-1291.

Hong, W., T.S. Chen, K. Y. Lin and W.C. Chiang, 2010. A modified histogram shifting based reversible data hiding scheme for high quality images. Inform. Technol. J., 9: 179-183.

Jurafsky, D. and J. Martin, 2000. Speech and Language Processing. Prentice Hall, Upper Saddle River, NJ., USA.

Li, J., R.D. Wang and J. Zhu, 2011. A watermark for authenticating the integrity of audio aggregation based on vector sharing scheme. Inform. Technol. J., 10: 1001-1008.

Liang, W., X. Sun, Z. Ruan and J. Long, 2011. The design and FPGA implementation of FSM-based intellectual property watermark algorithm at behavioral level. Inform. Technol. J., 10: 870-876.

Liu, Y., X. Sun, Y. Liu and C.T. Li, 2008. MIMIC-PPT: Mimicking-based steganography for microsoft power point document. Inform. Technol. J., 7: 654-660.

Liu, Z., X. Sun, Y. Liu, L. Yang, Z. Fu, Z. Xia and W. Liang, 2010. Invertible transform-based reversible text watermarking. Inform. Technol. J., 9: 1190-1195.

Ni, Z., Y.Q. Shi, N. Ansari and W. Su, 2006. Reversible data hiding. IEEE Trans. Circ. Syst. Video Technol., 16: 354-362.

Park, B., J. Park and S. Lee, 2009. Data concealment and detection in microsoft office 2007 files. Digital Investigation, 5: 104-114.

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

Rabah, K., 2004. Steganography-the art of hiding data. Inform. Technol. J., 3: 245-269.

Tian, J., 2003. Reversible data embedding using a difference expansion. IEEE Trans. Circ. Syst. Video Technol., 13: 890-896.

Topkara, M., C.M. Taskiran and E.J. Delp, 2005. Natural language watermarking. Proceedings of the SPIE International Conference on Security, Stenography and Watermarking of Multimedia Contents, January 17, 2005, San Jose, CA., USA., pp: 441-452.

Topkara, M., U. Topkara and M.J. Atallah, 2006. Words are not enough: Sentence level natural language watermarking. Proceedings of the ACM Workshop on Content Protection and Security, October 27, 2006, ACM Press, California, USA., pp: 37-46.

Wang, H., X. Sun, Y. Liu and Y. Liu, 2008. Natural language watermarking using Chinese syntactic transformations. Inform. Technol. J., 7: 904-910.

Yang, B., X. Sun, L. Xiang, Z. Ruan and R. Wu, 2011. Steganography in Ms Excel document using text-rotation technique. Inform. Technol. J., 10: 889-893.

Yang, Y., X. Sun, H. Yang, C.T. Li and R. Xiao, 2009. A contrast-sensitive reversible visible image watermarking technique. IEEE Trans. Circuits Syst. Video Technol., 19: 656-667.

Zeng, W. and Y. Wu, 2010. A visible watermarking scheme in spatial domain using HVS model. Inform. Technol. J., 9: 1622-1628.