Performance Evaluation of Natural Language Text Watermarking using Encryption Techniques

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 129
Number 3

Year of Publication: 2015

Authors:
Manmeet Kaur, Kamna Mahajan

10.5120/ijca2015906789

Abstract

Advances in communication technologies have made it easier to distribute and communicate information effectively. The increasing use of Internet has caused the information to be paperless and all the working to be electronic as compared to the conventional paper distribution. As the information is available on internet, it is liable to many kinds of threats like illegal copying, distribution, tampering, authentication etc. Till now, the electronic information can be secured by using different techniques like steganography, cryptography, watermarking. In text watermarking various techniques are implemented for English, Chinese, Turkish and Arabic language text using different methods. This paper includes an improved text watermarking technique for English language text documents. This paper proposes a technique which uses natural language components and UMARAM encryption technique. This study has focussed on grammatical rules like conjunctions, pronouns and modal verbs to generate encrypted watermark message. The performance of proposed technique is compared with AES encryption technique. It has been concluded that UMARAM algorithm is robust against content modifications and at the same time, is capable of detecting tampering attacks. The resulted
technique is tested over various text documents to check the effectiveness of the algorithm.

References

9. Mi-Young Kim, Osmar R. Zaiane, and Randy Goebel, “Natural Language Watermarking Based on Syntactic Displacement and Morphological Division”.
Zero-Watermarking Approach for Authentication and Protection of Sensitive Text Documents”.  

**Index Terms**

Computer Science  
Pattern Recognition

**Keywords**

Text watermarking, Copyright Protection, Security, Encryption, Tampering, UMARAM, AES, robustness.