*https://dx.doi.org/10.4314/jcsia.v25i2.12*

# THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATIONS
**Vol. 25 , No2, December 2018**

## ENHANCED DATA STORAGE SECURITY IN CLOUD BASED ON BLOWFISH ALGORITHM AND TEXT STEGANOGRAPHY

**Mabayoje M.A[1]. Ajao J.F.[2],Usman-Hamza F.E[1], Saheed Y.K[3] and Adeniran K.A.**

**[1]University of Ilorin, Nigeria.**
mmabayoje@gmail.com, usman-hamza.fe@unilorin.edu.ng, khadijahmaade@yahoo.com
**[2]Kwara State University, Malete.**
jumoke.ajao@kwasu.edu.ng
**[3]Al-Hikmah University, Ilorin, Nigeria.**
**kayodesaheed@gmail.com**

**ABSTRACT**
Cloud Computing (CC) offers a lot of services that are widely used in Information Technology. These services include sharing of data, information applications and infrastructure, cost reduction, increased storage and flexibility. Despites these services and benefits that CC provides to its user. However, unreliable security, data redundancy and disaster recovery are some of cloud computing challenges. With the existence and introduction of several data security technique, intruders or hackers do not relent in their efforts in developing means of accessing private and important data in the cloud. There are different approaches for securing data in the cloud such as cryptography, steganography, and digital watermarking and so on. This paper presents the combination of Blowfish algorithm (symmetric cryptography) and font properties text steganography to improve the security of data stored in the cloud. Blowfish as a fast and secure symmetric cryptography algorithm was used to change the readable secret data known as plaintext into unreadable format known as cipher text, and then text steganography was applied to the cipher text to change the visibility of the cipher text. The experimental results obtained showed that the proposed system provides reliable security for documents that are store in the cloud.

**Keywords:** Cryptography, Steganography, Digital Watermarking, Cloud Computing, Security.

## 1.0 INTRODUCTION

Cloud computing (CC) is becoming more popular and widely used in Information Technology. Cloud Computing is an internet based technology that deals with distribution of data, information, applications and hardware. However, cloud computing have some challenges, one of the major challenges that cloud users encounters while using the services is unreliable data security [1].

Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Presently, there are different modern approaches of securing data in cloud

computing, they are watermarking, steganography, cryptography and so on [2].Cryptography is a technique in the field ofmathematics related to aspects of computer and information security. Cryptography is used to protect data and information through the method of transforming or changing data and information from its original or readable format (known as plaintext) to an unreadable format known as cipher text [3]. There are different types of algorithm used for cryptography such as DES, AES, RSA, and Blowfish and so on. Blowfish algorithm is a symmetric block cipher with a 64-bit block size and variable key length from 42 bits to 448 bits [4]. According to [5], Blowfish is one of the fastest block ciphers which have being developed to date. The performance of Blowfish algorithm in terms of the throughput, processing time and power consumption makes it superior compare to other symmetric cryptography algorithms such as Advance encryption standard (AES), Data encryption standard (DES), RC4 and so on.

The term "Steganography" can be referred to as sending a secret message while hiding it existence [6]. Although, steganography is a security approach but it can also be used to complement cryptography. According to [7], to guarantee additional security to a stenographic communication, the message can be compacted and encrypted before being hidden in the carrier. Steganography are of four types namely image, audio, video and text steganography. In this paper, our focus in this study is on text steganography. Text steganography is the changing of the format of an existing text, words within a text, generating random character sequences or using context-free grammars to generate readable texts. Due to deficiency of redundant information which is present in image, audio or a video file, text steganography is believed to be the trickiest technique [8].

## 2.0 Related work

[9] presented a simulation result of the comparison between DES, Blowfish and AES in 2011. The result also shows Blowfish performs better compare to other common symmetric algorithms used. It was concluded that no security weak points has been identified so far for Blowfish algorithm which gives it high priority when it comes to selecting an algorithm.

In highlighting the strength of Blowfish algorithm, [10] work on the performance analysis of cryptography algorithms in 2014. It was concluded that the performance of Blowfish is better than AES, DESX in terms of encryption and decryption process of .EXE and .DOC file.

A novel text steganography system was proposed by [11]. In this approach, he used font color of the invisible character in Microsoft word documents to hide the visible characters. It was discovered that the capacity of the method is very high because it hides 3 bytes of data in every invisible character, and it was concluded that the method is a good choice for text steganography.

The authors in [12] investigates the security issues and challenges in cloud computing. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. Experimental analysis show that cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

The authors in [13] propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our schemeachieves the integration of storage correctness insurance and dataerror localization, i.e., the identification of misbehaving server(s).Unlike most prior works, the new scheme further supports secureand efficient dynamic operations on

data blocks, including: dataupdate, delete and append. Extensive security and performanceanalysis shows that the proposed scheme is highly efficient andresilient against Byzantine failure, malicious data modificationattack, and even server colluding attacks.

The authors in [14] implement a Steganography method using Unicode system characteristics in Ms- Excel document. The hiding capacity of their method is very high; they hide "1" bit in each number in Excel sheet because the approach has an excellent perceptual clearness because the stego text which the user sees is exactly similar to the original text. However, the approach is limited to hide data in electronic documents (e-document).

[15] implement a family of customized Cryptographic schemes known as Hiding by Symbols (HSym), Hiding by Coding (HCod), Hiding by Number (HNum), and Hiding by Phrase (HPhs) and Steganographic schemes Hiding by Meaning:(HMea), hiding by Abbreviations (HAbr), and Hiding by Emoticons (HEmt) for text hiding in OLST (online short text). These schemes are evaluated in terms of their security and their performance with regard to metric that address the particular characteristics of OLST hiding rate. In their research, all implemented schemes are proved to be at least computationally secure, and their performance in terms of hiding rate justifies their applicability in social networking tools that utilize OLST.

In [16], Khaurana & Gupta proposes a hybrid system for cloud security. RSA was used to secure User's Identification and Homomorphic was used for security of data. The method was very secure for both the user's identification and data on the cloud. Also, it has a great ease of use and versatility.

## 3.0 Proposed Method

The architecture of the propose system is show in figure 1. The architecture follows a steganography approach based on text steganography before the blowfish encryption is applied on the cipher text to obtain the secret document. The secure document is sent over the internet and the receivers decrypt the document.

The breakdown of the entire process of the method used in this study is stated as follows;

Step 1: Select and Extract content from secret document.

Step 2: Generate secret key using Blowfish.

Step 3: Apply Blowfish Encryption to the content extracted using the generated key.

Step 4: Select cover document and extracts properties.

Step 5: Determine the color of invisible character such as white space or paragraph from Step 4.

Step 6: Apply the font properties obtained in Step 5 to the cipher text.

Step 7: Append the invisible cipher text to the content of the cover document to generate a stego document.

Step 8: Send the stego document to the cloud.

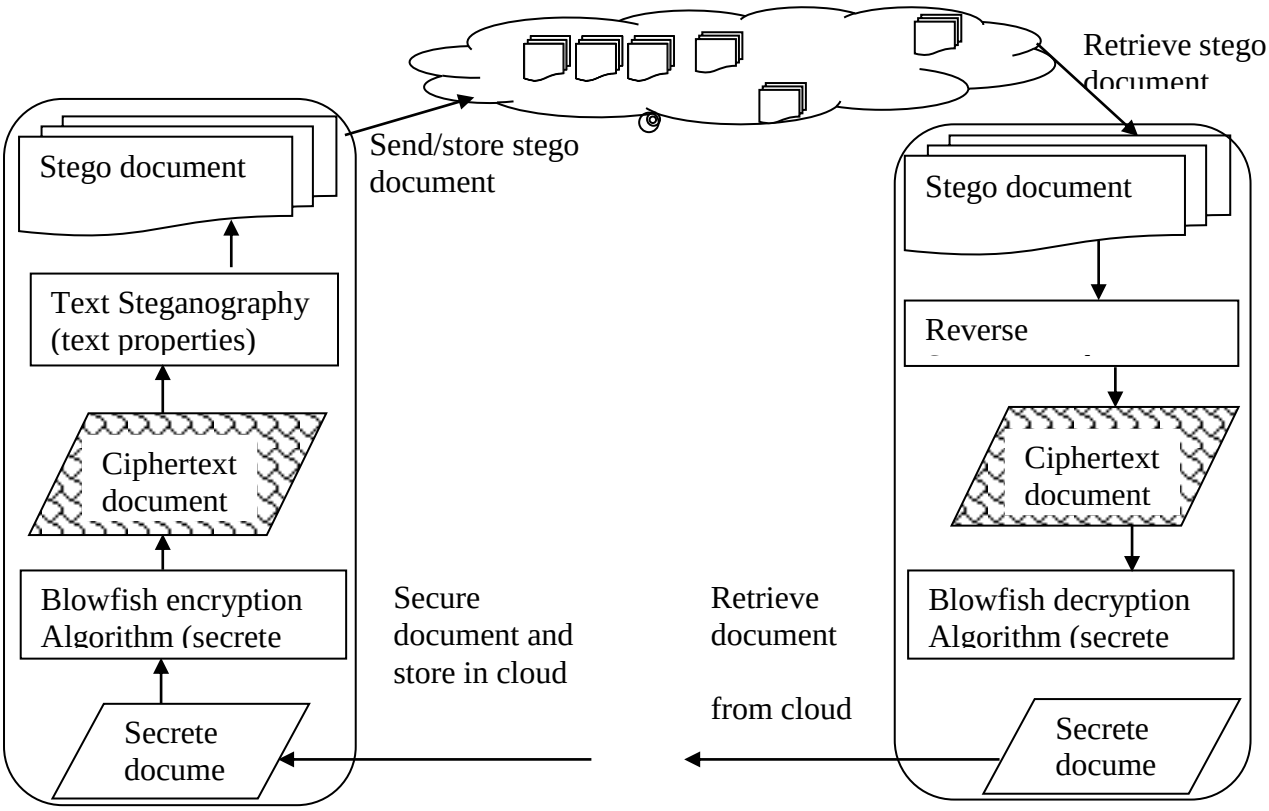



**Figure 1:** Architectural Design of the combined system

## 4.0 RESULT

The figures 2-9 shows the interface of the new developed system as well as the stego document generated




**Figure 2**: The Secure File Interface

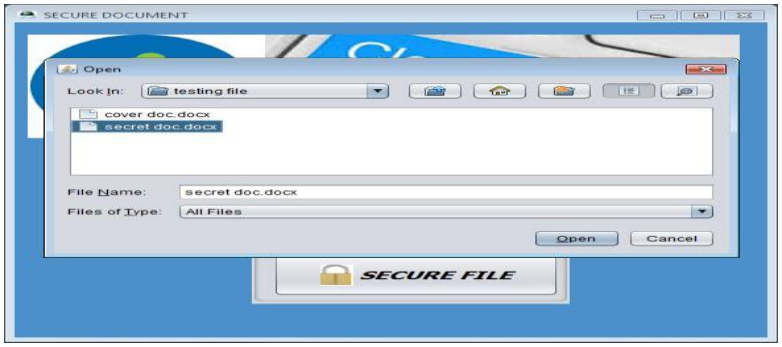



**Figure 3:** User selecting document to be secured




**Figure 4:** Document selected and ready for secure operation.




**Figure 5:**User asked to select the type for stego document




**Figure 6:**User enter name to identify the generated stego document

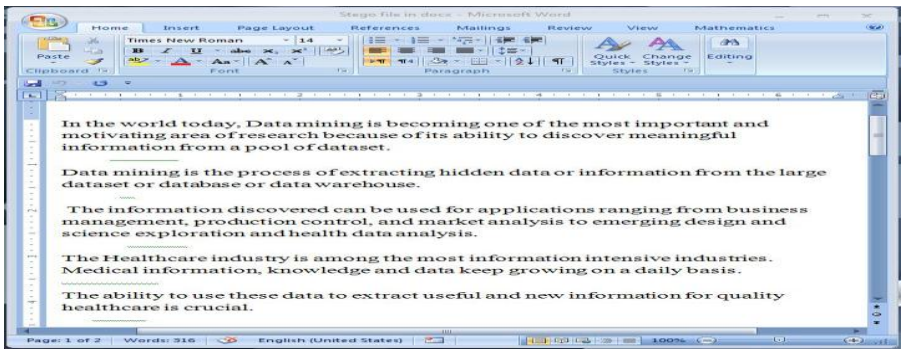



**Figure7:**Generated stego document in docx format




**Figure 8:** Generated Stego document in .docx with possible attack

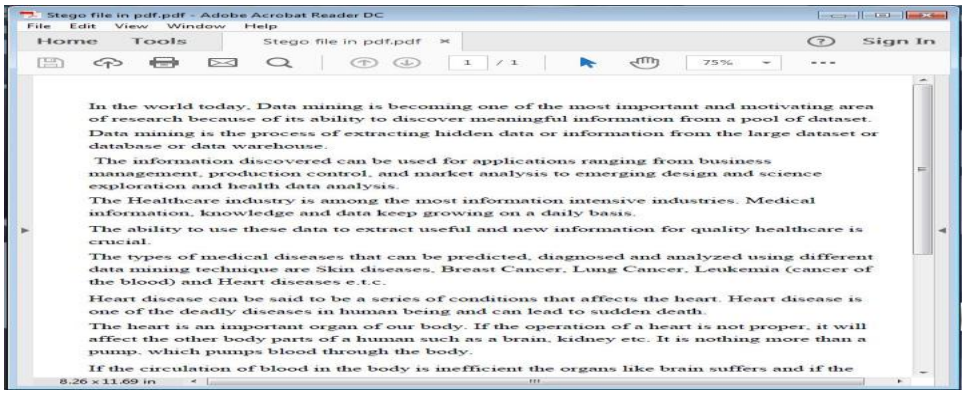



**Figure 9:** Generated stego document in pdf format

**Table 1:** The analysis and evaluation of result using generated stego document

| | **Size of File** | **Possible Visual Attack** | **Reliability** |
|---|---|---|---|
| Stego Document in docx format | Higher than pdf format but Lower than original document | Grammatical Error Attack, No of Pages, Words Count & Paragraph Gap | Very low |
| Stego Document in pdf format | Lower than both docx format and the original document | None | High |

## 5.0 CONCLUSION

The developed system provides a reliable security for document that is intended to be saved in cloud. The combination of cryptography and text steganography technique empowers the system and makes it suitable for use by both individuals and organizations irrespective of the sector. The text steganography help to increase the volume of information that can be hidden. Stego document of the combined system can be generated in .docx and .pdf format. However, the stego document generated in .docx is prone to visual attack such as number of pages, Grammatical Error Attack (GEA) and words count but stego document generated in pdf resist this visual attack which makes it a better choice to choose when using this combined system. The future study for this research would be to make use of Microsoft word document containing images and tables as well as other Microsoft document such as Excel, Power Point and so on needs to be address because this study only pays attention to Microsoft word document containing text only.

## REFERENCES

[1] Al-Khanjari Z. &Alani A.,(2014). Developing Secured Interoperable Cloud Computing Services. European Scientific Journal August 2014 edition vol.10, No.24 ISSN: 1857 – 7881 (Print) e - ISSN 1857-7431341

[2] Rosziati Ibrahim &Teoh Suk Kuan , (2011). Steganography Algorithm to Hide Secret Message inside an Image. Computer Technology and Application 2 (2011) 102-108

[3] Gabriel A.J., AleseB.K., Adetunmbi A.O. &AdewaleO.S., (2014). Post-Quantum Crystography based Security Framework for Cloud Computing. Journal of Internet Technology and Secured Transactions (JITST), Volume 3, Issue 4, December 2014

[4] AshwakAlabaichi, Faudziah Ahmed &RamlanMahmod (2013). "Security Analysis of Blowfish algorithm", IEEE, pp. 12-18, 2013.

[5] Minta Thomas &Panchami V., (2015). An Encryption Protocol for End-to-end Secure Transmission of SMS. 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT] 978-1-4799-7075-9/15/$31.00©2015 IEEE

[6] S.Samyuktha, C.Vijaya& D. Durai Kumar, (2015). Implementation of Key-Aggregate Cryptosystem with Steganography for Secured Data

Sharing In Cloud Computing. International Journal of Engineering Sciences & Research Technology (IJESRT) [Samyuktha, 4(3): March, 2015] ISSN: 2277-9655 Scientific Journal Impact Factor: 3.449 (ISRA), Impact Factor: 2.114 http: // www.ijesrt.com

[7] Khalil Challita and HikmatFarhat, (2011) .Combining Steganography and Cryptography: New Directions. International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208 The Society of Digital Information and Wireless Communications, (ISSN 2220-9085)

[8] K. Aditya Kumar , Dr. Suresh Pabboju&NeelaMeghaShyam Desai , (2014). Advance Text Steganography Algorithms: An Overview. . International Journal of Research and Applications. Jan-Mar © 2014 Transactions; 1(1): 31-35 ISSN (online): 2349-0020 http://ijraonline.com

[9] Jawahar Thakur &Nagesh Kumar, (2011). DES, AES and Blowfish Symmetric Key Cryptography Algorithms Simulation based performance Analysis. International Journal of Emerging Technology and Advanced Engineering.ISSN 2250-2459 volume 9, Issue 2, December 2011.

[10] RishabhArora&Sandeep Sharma (2012). Performance Analysis of Cryptography Algorithms .International Journal of Computer Applications (0975 – 8887) Volume 48– No.21, June 2012 35

[11] Md. Khairullah, (2009). A Novel Text Steganography System Using Font Color of the Invisible Characters in Microsoft Word Documents. 2009 Second International Conference on Computer and Electrical Engineering

[12] Kuyoro S. O., Ibikunle F. &Awodele O. (2011).Cloud Computing Security Issues and Challenges.International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[13] Cong Wang, Qian Wang, and KuiRen and Wenjing Lou (2013). Ensuring Data Storage Security in Cloud Computing.

[14] Aliea Salman Saber and WidAkeelAwadh, (2013). Steganography in Ms Excel Documen Using Unicode System Characteristics. Journal of Basrah Researches (Sciences)Vol.(39). No. ( 1) .A ( 2013 ). ISSN 2695 1817. Available online at: www.basra-science-journal.org

[15] AvinashChandragiri, Peter A. Cooper, Yanxin Liu &Qingzhong Liu,( 2014). Implementing Secure Communication on Short Text Messaging. 2nd International Symposium on Digital Forensics and Security (ISDFS'14), 12-13 May 2014, Houston, TX

[16] Rahul Khurana&Himanshu Gupta, (2016).A Hybrid Model on Cloud Security. 2016 5th International Conference on Reliability, Infocom Technologies and Optimization(ICRITO) (Trends and Future Directions).

## CONCLUSION

This work presented a malware detection system using Adaptive Neuro-Fuzzy Inference System. It was based on extracting both the API calls and N-gram inside each of the executable files. IDA Pro disassembler was used to disassemble the executable file and the result was passed into the database using a plugging called Ida2python and Ida2Sql. Features selection was used to prune down the number of our parameter to five. Those five parameters were used to train ANFIS, SMO, Naïve Bayes and Random Forest. As shown from the experimental result, the detection accuracy of ANFIS classifier outperform others classifier. This offers a promising approach in zero day attack detection. Since ANFSMD can deal with many of the zero day attacks, we intend to expand this approach to develop a self-healing based malware detection

## REFERENCES

[1] M. Alazab, S. Venkataraman, and P. Watters, Towards understanding malware behaviour by extraction of API calls . Cybercrime and Trustworthy Computing Workshop. 2010.

[2] A. Altyeb, A. Ammar and R. Sureswaran, Application of Adaptive Neuro-Fuzzy Inference System for Information Secuirty. Journal of Computer Science, 983-986 ISSN 1549-3636. (2012).

[3] A. Ammar, M. Elhadi, and H. Ahmed, Malware Detection Based on Hybrid Signature Behaviour Application Programming Interface Call Graph. American Journal of Applied Sciences, (pp. 283-288). 2012.

[4] S. Bradfield, A General Definition of Malware. J. Com. Virol., 6(2). 2010.

[5] K. Clemens, M. Paolo, K. Christopher, K. Engin, Z. Xiaoyong and W. XiaoFeng, Effective and Efficient Malware Detection at the End Host. TU Vienna: Secure Systems Lab. (2010).

[6] G. Erdelyi, Reverse Engineering III: PE Format, Loading a DLL from memory, 2010. [Online document] Available: http://www.joachim-bauch.de/tutorials/loading-a-dll-from-memory/. [Accessed: April, 2013]

[7] M. Eskandari, and S. Hashemi, A graph mining approach for detecting unknown malwares. Journal of Visual Language and Computing, 154-162. (2012).

[8] M. Eskandri, S. Hosseini and S. Hashemi, Malware detection using OWA measure. Journal of Computing, Volume 2, Issue12. (2010).

[9] T. Gil, R. Lior, and S. Yuval, Automatic Malware Detection Using Common Segment Analysis and Meta-Features. Journal of Machine Learning Research , (pp. 949-979). 2012.

[10] E. Goppit, Portable Executable File Format – A Reverse Engineer View. (2006).

[11] D. Harley, Making Sense of Anti-malware Comparative Testing (2010).

[12] Idapython. 2009. [Online]. Available: http://code.google.com/p/idapython/ [Accessed March 2014]

[13] J. Kolter, and M. Maloof, Learning to detect malicious executable in the wild. ACM SIGKDD International Conference on Knowledge discovery and Data Mining, New York, NY, USA. 2004. (pp. 470–478.).

[14] G. Mahboobe, S. Ashkan, and S. Zahra, DyVSoR:Dynamic Malware Detection Based on Extracting Patterns from Value Sets of Registers. The ISC Int'l Journal of Information Security, 2013 Volume 5, Number 1 (pp. 112).

[15] Microsoft Inc, "Portable Executable and Common Object File Format Specification". Implementation guide for PE files. Revision 8.2. MSDN Library.

[16] S. Mirza, K. Mat, and O. Zakaria, A

biological model to improve PE malware detection Review. International Journal of the Physical Sciences, 2236-2247 2010.

[17] R. Perdisci, A. Lanzi and W. Lee, Classification of Packed Executables for Accurate Computer Virus Detection . Elsevier, vol. 25. (2008).

[18] B. Potter and G. Day The effectiveness of anti-malware tools. Computer Fraud and Security , 12-13. (2009).

[19] R. Riley, X. Jiang and D. Xu, Guest-transparent prevention of kernel rootkits with Vmm-based memory shadowing. Proceedings of the International Symposium on Recent Advances in Intrusion Detection. (2008).

[20] R. Roshna and E. Vinodh, Adaptive Neuro fuzzy Inference system to predict the behaviour of bots. International Journal of Engineering Research and Applications (IJERA), (2013). 1440-1445.

[21] I. Santos, B. Felix, U. Xabier, and G. Pablo, Opcode sequences as representation of executables for data-mining-based unknown malware detection. Inform. Sci., doi:10.1016/j.ins. (2011)

[22] M. Schultz, E. Eskin, F. Zadok and S. Stolfo, Data mining methods for detection of new malicious executables. IEEE Symposium on Security, 2001. (pp. 38-49).

[23] Symantec, "Internet security threat report" [Online document], 2013 Volume 19. Available: Symantec Corporation Online www.symantec.com/.../en/.../b-istr_main_report_v19_212910118.en-us.pdf [Accessed

[24] P. Vinod, V. Laxmi, and M. Gaur, Survey on malware detection methods. Department of Computer Engineering, Malaviya National Institute of Technology 2009.

[25] VX Heaven, "Computer virus collection " [Online database]. Available: Malware Collection: http://vxheaven.org/ [Accessed: March 2014]

[26] W. Yan, Z. Zhang, N. Ansari, and T. Micro, Revealing Packed Malware. IEEE Security & Privacy, (2008). 65-69.

[27] Y. Ye, D. Wang, T. Li, and D. Ye, An intelligent pe-malware detection system based on association mining. Journal in Computer Virology, 2008. 323-334.

[29] Z. Zhao, G. Ahn, and & H. Hu, Automatic extraction of secrets from malware. Laboratory of security Engineering for future computing. Arizona state university. Tempe. (2011).

[30] Hex-Rays. Retrieved march 2014, from IDA: www.hex-rays.com/idapro/