

## Opponent's Report on PhD Thesis:

### *“Artificial Intelligence Applied on Crypto-analysis Aimed on Revealing Weaknesses of Modern Cryptology and Computer Security”, written by Eng. Jiří Hološka*

The dissertation theme is very interesting and high topical. The steganography is an art of invisible communication. Its goal is to send a secret message without raising any suspicion that the communicating parties want to hide something. The goal of the thesis is to *use artificial neural nets to detect message in JPEG digital images hidden by means of steganography*. The author suggests and solves numerous challenging questions for a high-quality PhD thesis. The unquestionable novelty of the dissertation work (written on 84 pages in 15 Chapters + 4 Appendixes on 33 pp. in English) is in the *design of features used as an input to the neural network*. Unfortunately, extremely little space is devoted to this main novelty of the work. "

The problem of this work lies in unjustified assumptions and in relatively incorrect experimental methodology. The author *should use state of the art methods*. From time to time it seems that since authors are not aware of it, they detect differences in quantization tables instead of steganographic attacks. Here, it has to be pointed out, that in most steganographic literature, these problems are covered and experiments are designed such that "double-compression" during embedding is avoided. The steganalytic method used in Section 9.6 is obsolete and it is not considered as a serious tools. *These all could lead to results, which are not credible always*. The visual quality of the thesis is also *poor*. The author did not even bother to write tables of his own results in consistent manner and not to use scanned tables only. Also plenty of typing errors and grammatical errors suggest that author had finished the work in a hurry. It is not clear why spellchecker has not been used. Similarly, the presented text and its structure should have been proof-checked prior to submission. - Overall, the quality of the dissertation thesis is low relatively. Despite the new presented method might work, it is not described in sufficient detail and the experimental methodology is not credible in all cases.

Reviewing the thesis was difficult for me because my expertise intersects with the thesis domain only in the area of Artificial Intelligence and Cybernetics which I have long-time experience from the Intelligent Robotics and Artificial Life side mainly. I feel to be an informed layman in Cryptology. Dr. Eng. Tomáš Pevný (working now at the same Dept) studied this topic in U.S.A. two years ago. He offered me that he will browse the thesis and will give me the opinion on it from the *Modern Cryptology and Computer Security Systems* perspective. He did it and I am grateful for that. From this cooperation the following observations, objections and questions have emerged. I believe you will respond to these problems fully.

- On page 17, and later on in Section 4.1.3, the author divides steganography into 3 classes. *Why the source of this division is not cited?*
- State of the Art described extremely short on two pages (17+18) is obsolete. The last citation is from 2003! As a consequence, several statements, most importantly that *“Artificial Intelligence has not been used in steganalysis”*, are not correct. The use of machine learning algorithms, through mostly *Support Vector Machines* and *Fisher Linear Discriminant*, is already well established within the field (*state of the art steganalytical tools*). *Respond to these facts!*
- The list of steganographic algorithms presented in Section 4.2 *is out-of-date and it is not complete*. *Advanced steganographic algorithms* such as Model Based steganography, Jp Hide&Seek, MMx, nsF5, YASS *are missing*. *Could you describe some features of these advanced algorithms briefly?*
- In short Section 6.2 you claim that *steganographic algorithms changes quantization tables*. *Is it always true? When this assertion is not valid?*
- The Experimental Section does not describe used methodology in such details that would allow reproducing of experiments. It is not clear, which quality factors were used during experiments, how cover and stego images were created, etc. *Under what assumptions you can repeat the experiment and achieve the same result?*
- The presented method, which should be the core of the dissertation thesis, is described on three and half pages only including 3 Figures and 1 Table. From the reviewed thesis it is absolutely not clear, how the method works and is in contrast with “reproducibility of research” paradigm. *Can you explain the used principles in more details step by step?*

- The authors claim that they are *able to detect 5 bytes long message hidden by F5 algorithm*. I am almost 100% sure that this is not possible. F5 algorithm uses powerful matrix embedding and my guess is that hiding 5 byte long message changes less than 8 DCT coefficients. *This is not detectable*. Although Figures 8 in the thesis shows that more coefficients are changed, this is caused by incorrect settings of the Experiment described above. *Could you react on it?*
- The used ANN topology is described by you on the page 48. *I would like to ask you, whether you have had a specific reason to choose a topology with two hidden layers?* See: <http://www.heatonresearch.com/node/707>
- The graph in Fig.1 on page 53 shows the course of training errors depending on the number of iterations. *In which iteration, i.e. on what basis, you decided to stop learning of ANN and use it for testing?* (My query is valid for all experiments performed by you!)
- *In which way was the data for training /testing divided?* It seems that the network was trained on completely different figures than on the figures upon which it was tested?
- *Did you try to teach the ANN on a universal detector of the hidden messages?* I mean to learn the network on some data generated using all available algorithms, and then evaluate the success of the detector on unknown data (i.e. either a modified image, or an image, modified by the used software)?
- *Do you expect success in the detection of a situation where ANN was learned on data generated by several well-known programs to detect pictures modified by a completely unknown program (i.e., when network “did not see” it by learning)?*
- This would be very interesting to compare detections. It is quite missing in the whole dissertation. *Could you present a briefly comparison during defence of your dissertation?*
- On page 69 you describe the best topology ANN found by you as the ANN with one neuron in the hidden layer. My question is: *Is a hidden layer needed in such case?*
- *What software was used for classification using ANN?* (This information is also missing in the whole dissertation.)

My weaker expertise in this highly specialized thesis domain forced me to look more carefully the impact of the PhD candidate's research in the scientific community through his publications. Regarding publications of Ing Jiri Holoska, the list of 14 items is relatively impressive. All titles were published during 3 years after his Diploma Thesis defending – since 2008. I could conclude that the reviewed work did not have a significant impact to the research community till now. - But this would not correspond to the reality! I can personally confirm that the author's papers presented at some prestige international conferences (as MENDEL 2009, ECMS 2010 and ECMS 2011) have always provoked great interest and their partial results have been very positively evaluated by the professional audience. The main contribution and novelty of this thesis is undoubtedly in the *original design of features used as an input to the neural network*. I have personal experience with programming, so I admire huge amount of hard work that is described and explained by author of dissertation thesis marginally only.

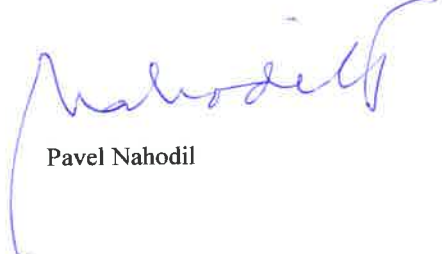
My decision about reviewed PhD thesis *oscillated between giving the negative and positive assessment* for a longer time. I will be *very open to the extensive discussion at the defence*. I inclined to the positive decision finally.

Despite the many remarks above, Ing Jiří Hološka has proved to be capable of solving new research problems. He has demonstrated in his work the ability to perform an experimental research and find new solutions. Mr. Hološka's Ph.D. thesis satisfies conditions of the Czech Act 111/1998 and its Section 47, and therefore

#### I recommend

his Ph.D. thesis to the State Committee to be presented and defended in the Technical Cybernetics study branch and, if the defence is successful, to award him the academic title “Philosophicae Doctor”, abbreviated Ph.D.

Prague 3. December 2011



Pavel Nahodil

## **Examiner's report of doctoral thesis**

**Author:** *Ing. Jiří Hološka*

**Title:** *Artificial Intelligence Applied on Cryptanalysis Aimed on Revealing Weaknesses of Modern Cryptology and Computer Security*

**Examiner:** *Doc. RNDr. PaedDr. Eva Volná, PhD.*  
*University of Ostrava*

### **Objectives of the thesis and their fulfilment**

A given doctoral thesis concerns the issue of steganography detection using graphical format as a carrier medium. The doctoral student chose programs - OutGuess, Steghide, CipherAWT (F5 algorithm) and PQ, which included the steganographic content (hidden messages) into figures. Whole detection is performed using artificial neural networks in several different topologies. The chosen method can be considered as fully competent and it is sufficient for purposes and objectives of the PhD thesis. This is about artificial neural networks, which are included into the "softcomputing" area. It is possible to certify that the topic of the thesis is up-to-date.

The given thesis has fulfilled its main objectives and contains a great effort that was also reflected in the author's publication activity.

### **Benefits in the field of knowledge**

The thesis deals with the detection method based on artificial neural networks. Its objective is to minimize or completely eliminate inaccuracies in classification. The research is focused on the detection of hidden information in multimedia files, especially in images, using some steganography method. The chosen methodology of data processing is one of the author's benefits. To achieve results presented in the work, author developed his own software system. Experimental results bring a new view into the field of data processing using neural networks.

A range and a the quality of author's publications are satisfactory. In the years 2008-2011, he published 14 articles in journals and at international conferences and workshops.

### **Benefits in the field of social practice**

The author created an application, which demonstrates that the proposed method based on artificial neural networks is suitable for detection of stenography content in images. It is obvious that the proposal is based on good author's knowledge and experience with an implementation of similar problems in practice.

### **Formal arrangement**

The doctoral thesis has 84 pages and four appendixes containing tables of experimental results. Appendixes represent results of different settings of artificial neural networks presented in the thesis.

The whole thesis is written in English. The thesis is written and structured in a logical and well arranged way. Its text is presented at an appropriate level of expertise and it is compact. I have only comments on the quality of English. As regards the structure of thesis, it contains an introduction, state of art, a description of using methods and an experimental

study. The proposed procedures and methodologies are supported by copious publications of the doctoral student.

### **Questions and comments**

I would appreciate more detailed state of art. I miss more references to current work. Only a quarter from 49 cited items is less than 5 years old.

I have the following questions:

1. I miss a more detailed state of art. Could you briefly specify whether a given issue has been solved by other softcomputing methods too?
2. One of the objectives of thesis was to test a successful rate of neural network detector against the linear classification. Could you comment your achievements?
3. How did you set a neural networks topology in your experiments?

### **Conclusion**

The submitted thesis fulfils the requirements for a doctoral thesis, both in terms of theoretical - methodological level, so the usefulness in practice. The thesis contains the original results.

I recommend the thesis to the defence before the relevant commission. Based on the thesis, I suggest the academic and scientific degree "Doctor Philosophiae" (Ph.D. abbreviation) to confer to Ing. Jiří Hološka after successfully defending of his thesis.

Ostrava, 17 October 2011

Doc. RNDr. PaedDr. Eva Volná, PhD.



## Oponentní posudek disertační práce Ing. Jiřího Hološky „*Artificial Intelligence Applied on Cryptanalysis Aimed on Revealing Weakness of Modern Cryptology and Computer Security*“

Disertační práce Jiřího Hološky, jak nakonec napovídá i její dlouhý název, se zaměřuje na slabá místa v počítačové bezpečnosti a zabývá se návrhem metod pro odhalování informací vložených do multimediálních souborů, zejména obrázců, které při předávání mailů umožňují snadné a přitom skryté předávání nežádoucím způsobem zjištěných neveřejných firemních či obchodních informací.

Vzhledem k závažnosti tématu v dnešní době je výzkum v této oblasti aktuální a současně lze konstatovat, že jednoznačně spadá do okruhu problémů studovaných v oboru Inženýrská informatika, před jehož komisi doktorand svou práci předložil.

Prvních sedm kapitol práce je stručným popisem teoretických základů zkoumané problematiky, autor v nich vysvětluje steganografické metody pro vložení informace do souborů, speciálně do obrázků formátu .JPEG, a také principy neuronových sítí, které jsou využity k detekci. Zatímco u teorie steganografie doktorand zmiňuje i její historii (příklady ze starého Řecka, uplatnění steganografických metod v 2. světové válce), neuronové sítě, jejichž využití je přitom těžištěm disertace, pojednává velmi stručně až povrchně na třech stranách (str. 46-48).

Hlavním výsledkem práce jsou kapitoly 8 až 10, které popisují experimentální část a dosažené výsledky testů. Je třeba však říci, že i zde nelze najít detailní informace o použitých neuronových sítích a jejich učení. Popis je dosti povšechný, např. *bylo použito 1 až 20 neuronů ve skryté vrstvě a 9 kombinací přenosové funkce neuronu*. Je třeba ale říci, že detekční schopnost implementovaných metod je u všech čtyřech použitých programů (OutGuess, Steghide, CipherAWT (F5 algorithm) a PQ) téměř 100%-ní.

K práci mám několik připomínek:

- Není zcela zřejmé, co je vlastním přínosem autora, protože všechny jeho publikace, z nichž práce vychází, jsou kolektivním dílem většího počtu autorů.
- V cílech práce na str. 10 autor uvádí, že se pokusí optimalizovat délku vstupů do neuronové sítě a snížit její složitost. Není jasné, co myslí délkou vstupů a k čemu dospěl. (Jde o redukci vstupního vektoru trénovacích množin pro neuronovou síť, jak se o tom píše na str. 74?)
- Práce je napsána v angličtině, autor si však asi nezapnul jazykový korektor, protože jinak by musel řadu překlepů odhalit. Jen namátkou několik příkladů z úvodu textu: „Informatinon“ místo „Information“ na str. 13; obdobně „belongé“ – „belongs“ – str. 17; „discovering“ – „discovering“ – str. 17; „proces“ – „process“ – str. 18; „can be use“ – „can be used“ – str. 22; „the program use specific drivers“ – „the program uses ...“ – str. 27; „embedding“ a „embedding“ místo „embedding“ na str. 26; „the secret data is compressed“ – „... data are compressed ...“ – str. 27, atd. Zarážející je pak to, že ve všech tabulkách na str. 60-67 je uvedeno slovo „classification“ ve zkomolené podobě „classificaiton“, aniž by si to autor všiml, což nesvědčí o velké pozornosti závěrečné korektuře textu.

### **Dotazy na disertanta:**

1. Můžete blíže popsat učící algoritmus neuronové sítě a jak je zvolena strmost sigmoidy realizující přenosovou funkci neuronu?
2. Byly, resp. budou vaše programy nasazeny i v praxi?

### **Závěr:**

I přes velmi úsporný výklad je předložená disertační práce fundovaným dílem, které kriticky hodnotí výhody a nevýhody známých metod při řešení konkrétních problémů odhalování vynášení firemních informací, které mají charakter obchodního tajemství. Významným přínosem je realizační část práce, jejímž výsledkem jsou čtyři programy s velkou schopností detekovat skrytou informaci.

Domnívám se, že Ing. Jiří Hološka prokázal schopnost a připravenost k samostatné činnosti v oblasti výzkumu a vývoje, jeho disertační práce splňuje podmínky § 47 Zákona o vysokých školách č. 111/1998 Sb., její podstatné části byly publikovány (a také citovány) na mezinárodním fóru, a proto ji

### **doporučuji k obhajobě**

před komisí studijního oboru Inženýrská informatika

V Brně dne 15. února 2012



Prof. RNDr. Ing. Miloš Šeda, Ph.D.  
Ústav automatizace a informatiky  
Fakulta strojního inženýrství VUT v Brně