INFORMATION OF DOCTORAL DISSERTATION

Title of Thesis: **Study on methods to secure hidden information in digital photos**

Major: **Telecommunications engineering**

Code: **9.52.02.08**

Ph.D candidate: **Le Hai Trieu**

Research Supervisors: **Prof., Dr.Sc Do Trung Ta**

Training institution: **Posts and Telecommunications Institute of Technology**

NEW SCIENTIFIC FINDINGS

- First contribution: This candidate has proposed a new algorithm for information hiding using the 5-bit code set, which lists some following advantages. *Firstly*, it has reduced the embedding rate to approximately 3.2% (≈ 1/31). This is the ratio that allows for prevention of statistical attack algorithms at level 1 and level 2. *Secondly*, the aforementioned algorithm simplifies the embedment and extraction, besides, the amount of hidden information is larger with the LSB changing much less. *Thirdly*, it increases the ability to hide information. *Fourthly*, the use of 5-bit code word will encode all 26 Latin characters. Results of evaluation and comparison between new proposed algorithms and old algorithms show that the amount of hidden information is 60% higher than that of the old algorithms, PSRN ratio is higher than the permitted standard (> 38dB) and higher than the old algorithms (at least 64% with the same amount of hidden information), also the embedding rate is below 2% at the same time.

- Second contribution: This candidate has applied new pseudorandom bit generator algorithm with maximum cycle by linear congruent method with the purpose of exchanging secret keys for hiding information in digital photos. The three advantages of the new algorithm are shown as follows. *Firstly*, the R cycle of the sequence will be controlled if the Assumption 2's theory is correctly implemented; *Secondly*, the key exchange is very simple, which only needs 4 parameters x_0,*a*,*b*,*m*. It depends on the application's requirements to select a suitable *m*. This is the recursive formula to find the sequence $\{x_n\}$ with $n \geq 2$. *Thirdly*, this algorithm is used to exchange the cryptographic key for the aforementioned 5-bit algorithm by a public key cryptosystem; to be directly applied for contents in Chapter 4 as well as in defense and security studies.

- **Third contribution**: From the methods to assess the quality of hiding information and pseudorandom key generator, this candidate hereby proposes some methods to assess security and safety. *Firstly*, the quality of pseudo-random sequence generated from certain systems will be achieved if the components of that sequence are independent and evenly distributed. Thus, this dissertation introduces an algorithm to assess safety for pseudorandom bit generator systems and safety assessment algorithms for pseudorandom Latin alphabet sequence systems. *Secondly*, the method of perfect safety assessment is used through Kullback–Leibler divergence between the probability density function $D(P_s \| P_c)$. It has proposed the algorithm to evaluate function D which solves issues more simply and effectively with the evaluation result of $D(P_s \| P_c)$ divergence ≤0.05 and the safety rate of more than 98%.

- Fourth contribution: Based on the research, evaluation and comparison of JPEG / JPEG2000 being marked with watermark security, this candidate hereby draws a conclusion. *Firstly*, the author provides an analytical model and a numerical result describing the error

performance for the proposed model during the process of image processing according to JPEG / JPEG2000 standard and the process of securing watermark to corresponding sensor data. *Secondly*, this probability depends on the varying parameters such as the average watermark magnitude, the probability of false alarms, compression factors, image sizes and the block division for each image. *Thirdly*, securing digital photos by watermarking with DWT method is the best choice for both the error performance problem as well as the probability of finding watermark marks.

- **Fifth contribution:** Based on the lowering of network performance during common attacks, the dissertation proposes a model of Back-off algorithm state, channel state model, and 03 performance parameters. *Firstly*, a new analytical model has been proposed for IEEE 802.11 MAC layer by using EIED algorithm which includes handling back-off freezing. *Secondly*, it analyses network performance according to different back-off algorithms based on 3 parameters of traffic flow, packet drop probability and access latency for normal node and error node. *Thirdly*, the EIED back-off algorithm has been evaluated to have better performance than the BEB algorithm under common conditions. However, when the network has a poison node due to the effects of common attacks, its performance is better using the BEB back-off algorithm than EIED algorithm.

- **The sixth contribution:** Based on the actual work requirements and the above-mentioned research content, the dissertation has designed a professional secret communication system through digital image transmission with security according to the research above and FHSS digital transceiver module.

PRACTICAL APPLICABILITY AND OPENING ISSUES FOR FURTHER STUDIES

Currently, the methods of securing information in digital photos in particular and in digital multimedia products in public and secret communication are always attracting much attention and investment for research and development by many countries, especially by defense and security contractors. From this point forward, Ph.D candidate will continue to develop the following contents:

- Improving confidential information hiding algorithm to reduce information hiding rate to below 1%.

- Hardening pseudo-random number parameters to increase processing speed as well as key safety level.

- Doing research on the watermark security marking algorithm on multimedia.

- Improving network performance to prevent attacks by special methods.

- Continuing to complete professional secret communication system via digital image transmission with security as well as related accreditation procedures and records for use in actual work.

Research Supervisors	**Ph.D candidate**
Prof., Dr.Sc Do Trung Ta	**Le Hai Trieu**