International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 8, No.5 (Sep-2019)
http://dx.doi.org/10.12785/ijcds/080507

Real Time Implementation of Stegofirewall System

Muthana R. Al-Sultan [1], Siddeeq Y. Ameen[2] and Wafaa M. Abduallah[3]

[1] *College of Engineering, University of Baghdad, Baghdad, Iraq*
[2] *Quality Assurance Directorate, Duhok Polytechnic University, Duhok, Iraq*
[3] *Department of Computer Science, Nawroz University, Duhok, Iraq*

Received 16 Feb. 2019, Revised 7 Jul. 2019, Accepted 28 Aug. 2019, Published 1 Sep. 2019

Abstract: Great efforts made to detect secret hidden information within digital files. Unfortunately, these efforts are consuming large amount of time and may fail if the hidden information encrypted. Therefore, destruction of such hidden information using a stegofirewall filter seems to be the most appropriate solution. However, it is essential that such process should not affect the cover image file and any authentication information such as watermarking. The paper presents the design of a firewall system that passes the digital image files (the carrier cover) together with a watermarked image file and rejects the hidden content. The system will also achieve cover image enhancement since its operation relies on denoising filtering. This stegofirewall should have a processing speed compatible with that of high speed Internet. The latter requirement achieved through the hardware implementation of such a system using an FPGA to provide the real time speed limitations required. The system implemented using Matlab together with Spartan 6 and Virtex 5 FPGA chips. The results of Matlab simulation show that the system performs well in destruction, whereas the real time implementation shows that Virtex 5 is better than Spartan 6 for the real time implementation and within the acceptable time required.

Keywords: Denoising, FPGA, Stegofirewall, Watermarking

1. INTRODUCTION

Terrorists and cybercriminals are trying to benefit from security characteristics, which are available, intentionally or unintentionally over communications systems, while security authorities try to restrict terroristic and cybercriminals activities. One of the security techniques used by such criminals is steganography [1][2]. Thus, governmental authorities are often trying to overcome such threats. Moreover, it is a well-known fact that many international terrorist organizations and competitive military agencies assured to have benefited from steganography as mentioned in USA TODAY newspaper [1] [2] [3].

Great efforts used to find mechanisms the existence of secret information within digital files. Unfortunately, many of steganography files are not detectable. Furthermore, the hidden messages may be encrypted and consume large times in interpretation attempt making the attacks on steganography files very difficult in real time. Therefore, the steganalysis system is not enough for investigating the idealist aim, but the possibility to prevent the hidden message's arrival to the intended party. These have set up the research aims to find new mechanisms of security that has the ability to stop steganography threats and to implement the proposed solution in real time [4].

Thus, the scope of this research is to:

- Design a firewall system with the ability to disable steganography threats within digital image files after removing noisy steganography content
- Enhance carrier cover quality in addition to pass watermarked image files successfully.
- Make processing speed compatible with that of high speed Internet.
- Real time implementation of the steganography content destruction technique using FPGA hardware chip to provide the speed limitations required.

2. STEGOFIREWALL SYSTEM

A firewall is a hardware or software solution implemented within the network to enforce security policies suggested by an organization [5] [6]. The firewall is located between the public networks (Internet) and private networks where it inspects the traffic according to the predefined policy, and allowing only legitimate traffic to pass while the harmful traffic is disabled [5][7], as illustrated in Fig (1). There are some common characteristics or rules among various types of firewalls as follows [6]:

E-mail: muth85cnet@uobaghdad.edu.iq, Siddeeq.ameen@dpu.edu.krd, wafaa.mustafa@nawroz.edu.krd

- All traffic from inside to outside or from outside to inside must pass by the firewall.
- Legitimate traffic passes successfully while non-legitimate traffic rejected relying upon predefined rules by the intended security policy [8].
- A firewall has robustness against penetration and intrusion using an authenticated operation system.

In this research, a new component of a firewall, has been designed and implemented, to scan and clean the suspected image files. These suspected files include steganography that considered as a type of noise. Therefore, removing or disabling such type of hidden information using content destruction will enhance the image file's quality.

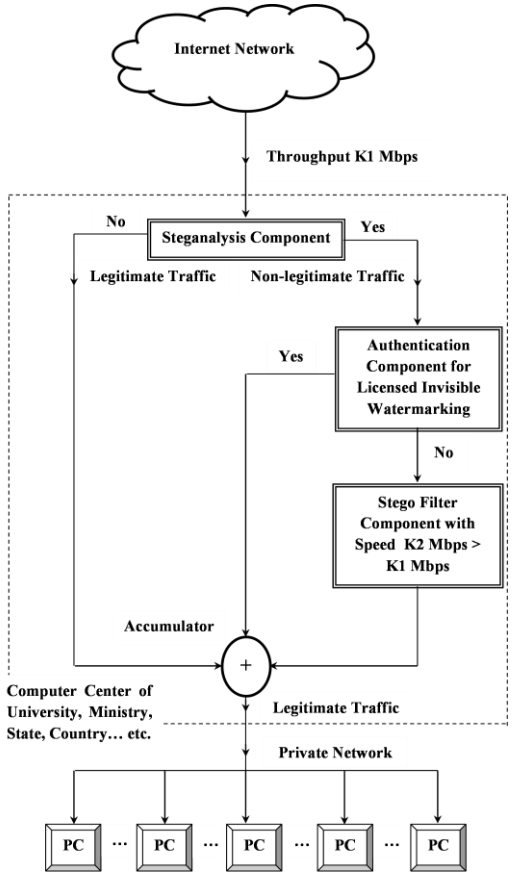


Figure 1. Block Diagram of Proposed Firewall System.

The philosophy of stego content destruction is different from other steganalysis branches. With such philosophy, any embedded information within digital medium for any type of steganography techniques destroyed. There is a small number of researchers that paid attention to such type of research, disabling and destroying steganography content within the digital multimedia files. In 2006, F. Al-Naima, et al, presented a new idea for destroying stego content inserted within digital image files using denoising technique based on discrete wavelet [3]. Next, William Jamieson suggested methods for steganography filtration. These methods classified into two types; dissolving and overwriting. Dissolving method has the ability to modify the image's pixels to make the decoding process of the stego image impossible. While in Overwriting, a new message is written again over original secret message within stego image files. For this reason, the hidden message is destroyed without leaving any noticeable modifications [4].

Extra studies conducted by Moskowitz, shows a new method called Stego Scrubbing. The architecture of this method has the ability to remove steganography. The philosophy behind such as this architecture is to build a filter or guard against steganography [9]. The research of discrete wavelet extended by Al-Terki was to investigate several filtration techniques of stego information in digital images such as compression and scaling. These techniques destroyed the hidden information partially or totally for any used technique of steganography [10]. Finally, Ameen and AL-Badrany presented two approaches for destroying steganography content in digital image files. The first is the overwriting approach where a random data written again over stego image files, whereas the second approach is the denoising approach. With the second approach two kinds of destruction techniques adopted, these are filtration and discrete wavelet techniques. The image filtration investigated in spatial domain, such as Mean Filter, Hybrid Filter and Wiener Filter. The wavelet investigated in transform domain, such as Bayes, Visu and Sure thresholding technique. These approaches have been simulated and evaluated over two types of hiding techniques, Least Significant Bit LSB technique and Discrete Cosine Transform DCT technique. The results of the simulation show the capability of both approaches to destroy the hidden information without any alteration to the cover image except the denoising approach enhance PSNR in any received image (cover image only) by an average of 4dB [11].

The research has shown that it is possible to destroy any hidden information in image files with the following noise effect in hiding and destruction;

- Denoising approaches destroy stego content because of their possibility to remove various noises from image files. For this reason, reverse steganography algorithm cannot retrieve secret message from stego image file as well as the image quality will be enhanced.
- Noise removal or rims blur will firstly target secret message length or stego key, if found. This is shared

between intended parties in addition to targeting other parts of the image file.

- Mean filter and Bayes-Shrink thresholding techniques are the best methods in stego destruction and cover quality enhancement when compared to other methods that investigated in this research. However, the optimal image stego content destruction technique is Mean Filter.
- Overwriting approach is very successful in preventing the secret message from being restored. However, this approach is working well with specific steganography technique such as LSB or DCT technique while it may be not compatible with other techniques of steganography. For this reason, denoising approach is much better than overwriting approach.

The optimal type of filter is the Mean Filter. It guaranties removing hidden information with other noise as well as enhancing carrier cover quality. This type of filter chosen to represents the proposed stegofirewall system.

Despite, that the research has shown remarkable performance in hidden information destruction, the research faced two problems. The first one is the speed requirements in image processing that makes the proposed system to be as a firewall in matching with the certain network speed. The second problem is the invisible watermarking system. The watermark might be destroyed or disabled as it passes through the proposed firewall. This problem occurred because the invisible watermarking system may represent a subset of steganography and can considered as a threat on the Internet.

3. WATERMARKING PROBLEM PROCESSING

There are two kinds of watermarking: visible and invisible watermarking. The first kind is the most used which is confusing a certain pictorial watermark with the carrier file to prevent unauthorized copyrights [12]. The visible watermarking achieved by merging the watermark image with the RGB cover image [13] where each color channel has been treated separately. Mathematically, the forward and reverse algorithm of the visible watermarking can be represented by equations (1) and (2), respectively.

$$\boldsymbol{I_{cw} = K_1 * I_c + K_2 * I_w} \quad (1)$$

$$\boldsymbol{I_w = \frac{(I_{cw} - K_1 * I_c)}{K_2}} \quad (2)$$

where K_1 and K_2 are transparency parameters, *Ic*, *Iw* and *Icw* is the cover image file, visible watermark image file and copyrighted watermarked image file, respectively.

The second type, invisible watermark, means hiding secret data such as a serial number inside the cover file to protect or authenticate the carrier cover file. Thus, this process can be considered as a subset of steganography. For this reason, the invisible watermarking system has the same embedding algorithms as that employed with steganography. The only difference between them is that the invisible watermarking has more robustness than steganography. This is because the embedding algorithms in transform domain provide more robustness against various attacks and the secret data (watermark) such as a serial number is mostly less than the hidden secret data (message) in steganography where embedding algorithms in spatial domain are used. Thus, the secrecy of steganography system will be more fragile than the invisible watermarking system. As a result, the investigation of steganography based on transform domain technique can represent the investigation of the invisible watermarking system. Furthermore, watermarking robustness is the most important requirement to overcome various attacks and restoring properly [13].

Authentication component is necessary in firewall design. There are many techniques of authentication such as user name or password (serial number) [14] [15]. Group of serial numbers is put in lookup table or directory of the firewall. This component of firewall inspects whether the suspected file contains a serial number or not, and then this serial number is compared with other serial numbers contained in the lookup table to grant the authentication as shown in Fig (1). This process is very essential especially with invisible watermarking to disable the invisible watermarking threats.

The invisible watermarked files contain predefined serial numbers relying upon a set of rules. This serial number or password related to firewall system and different from that used for authentication purposes between intended communication parties. This means that invisible watermarked files contain two different serial numbers (hidden information) for two different purposes. The serial number of suspected (invisibly watermarked) file licensed only when found in the directory of authentication component. This component does bypass for licensed files. For this reason, the licensed invisible watermarked files passed successfully without any effect over the proposed firewall system. However, unlicensed invisible watermarked files are filtered exactly in the way as steganography files.

Finally, the serial numbers of the lookup table or directory in the authentication component installed and updated by the governmental authorities or Internet officers.

4. REAL TIME IMPLEMENTATION USING FPGA

The real time implementation problem of stegofirewall arises because of the large amount of data to be processed. The hardware technology of parallel processing considered as one of preferred solution. This can be achieved using FPGA technology since its devices have advantages of achieving task-level implementation of the parallel, which greatly accelerate the speed of calculation [16][17]. Moreover, these real time applications require that the throughput of incoming data to any processing system such as denoising system is similar to the throughput of outgoing data from that system. On the other hand, modern versions of FPGA have huge possibilities for processing in parallel so they are very appropriate when treating with image processing designs. Furthermore, FPGA chips can be reprogrammable, until at implementation time, investigating the requirements of a certain design. Therefore, one chip can implement a number of various applications. However, memory resources of modern FPGAs are limited, so some designs are restricted in practical application, especially for image processing designs. Furthermore, FPGAs have poor processing ability compared with DSPs, when implementing computations in sequencing [17]. Consequently, the real time implementation using FPGA needs to be achieved efficiently and inexpensively.

Since, the optimal stego content destruction technique achieved by the Mean Filter MF. Thus, this filter is chosen to be implemented with FPGA chips using Very High-Speed Integrated Circuits Hardware Description Language VHDL written in Integrated Software Environment ISE version 14.1. Furthermore, the image processing must be processed in parallel with speed matched to the speed requirements. In the FPGA implementation, Spartan 6 XC6SLX16 and Virtex 5 XCVSX50T are used. The processing speed of these two chips are 200 MHz and 100 MHz, respectively.

In the implementation, it was assumed that the proposed stego filter component applied to a sample of RGB Lena image file with size (8x8) pixel because FPGA memories are limited. The sample of Lena image file corrupted by stego (noisy) content using LSB and DCT steganography. The distributed RAM memory used to store the stego image file before and after processing.

Finally, it is worth to mention that the implementation can be applied to video signals. This is because video signal processing requires processing more than 30 frames per second [18]. In the implementation, it has been found that the speed of proposed firewall components has to be matched with each other and minimum speed has to be more than or equal to the network speed that required to be filtered.

5. SYSTEM SIMULATION AND EVALUATION

The optimal stego image content destruction technique that adopts the Mean Filter has been implemented and simulated. The system evaluated in terms of denoising performance together with the condition of hidden information destruction. Thus, the Bit Error Rate BER and the Normalized Correlation NC between the original watermark and extracted watermark are used to measure the robustness characteristic of watermarking. Mathematically, the BER and NC are calculated using [19]:

$$BER = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} w(i,j) \oplus w'(i,j)}{M.N} \quad (3)$$

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} w(i,j).w'(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} w(i,j)^2}\ \sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} w'(i,j)^2}} \quad (4)$$

where $w(i,j)$ is an original watermark bit, $w'(i,j)$ is extracted watermark bit and M, N are the watermark size. It is well known, that the BER and the NC values are generally 0 to 1 and the ideal values for the BER and the NC should be 0 and 1, respectively.

The results presented in Table I show the effect of applying steganography filter (mean filter) component of proposed firewall system on the robustness of invisible watermarking. These results assume the usage of repetition code (1, 5) approach in watermarking since the highest robustness achieved. Furthermore, the evaluation considers subjective and objective measurement. The first measurement achieved via the measurement of the BER and the NC. The results show that the repetition code technique fails to protect invisible watermarked content from destruction. This is because invisible watermarking is a subset of steganography. However, the results shown in Table II illustrate that only visible watermarking system passes successfully without any harm but its quality will enhance if the noise is present exactly as same as its carrier file. This is because the proposed firewall system considers the watermarks as a part of the carrier file.

TABLE I . PASSING INVISIBLE ROBUST WATERMARKING SYSTEM BASED REPETITION CODE (1,5) APPROACH OVER PROPOSED FIREWALL SYSTEM IN TERM OF: (A) SUBJECTIVE. (B) OBJECTIVE.

(A)

Subjective Measurement	*Before Applying Firewall*	*After Applying Firewall*	
		Without Method	*Repetition Method*
BER	0	0.4794	0.4349
NC	1	0.6633	0.7013

(B)

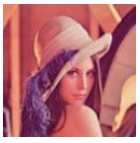
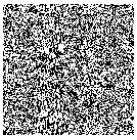
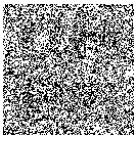
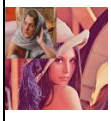
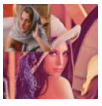
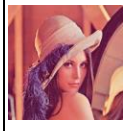
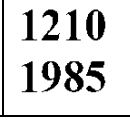
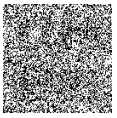
Objective Measurement	*Before Applying Firewall*	*After Applying Firewall*	
		Without Method	*Repetition Method*
Invisible Watermarked Image			
Extracted Invisible Watermark			

TABLE II. PASSING VISIBLE AND INVISIBLE ROBUST WATERMARKING SYSTEM OVER PROPOSED FIREWALL SYSTEM

Objective Measurement	*Visible*		*Invisible*	
	Before Firewall	*After Firewall*	*Before Firewall*	*After Firewall*
Watermarked Image				
Extracted Watermark				

The investigation also considers firewall performance with video signals. The video signal need to be processed more than 30 frames per second. For this reason, the following equations adopted to calculate the number of processed frames per second:

$$F = \frac{1}{T_p x\, S_i} \quad (5)$$

$$T_p = \frac{T_s}{S_s} \quad (6)$$

where F is the number of frames per second, Tp is the processing time of each pixel, S_i is the size of image file, Ts is the processing time of the sampled image that is calculated using ISim Simulator and S_s is the sample size of image file.

Extra investigation essential for real time is that the proposed firewall need to have a processing speed more than or equal to the network speed. This is usually verified by measuring the throughput of stego filter component given by:

$$Throughput = \frac{8}{T_P} \quad (7)$$

In the evaluation, RGB Lena image file with BMP format and size (256x256) pixel have been adopted and processed using PC software with a processor (Core i3-2.10 GHz). The PC software is a Matlab program 2012a where the software execution time was equal to 16.354 seconds. Furthermore, the same image file has been processed using FPGA hardware chips. The speedup can be achieved by [20]:

$$\boldsymbol{Speedup} = \frac{Software\ Execution\ Time\ Using\ Matlab}{Hardware\ Execution\ Time\ Using\ FPGA} \quad (8)$$

In the two cases (models) of FPGA, the three colors (red, green and blue sample) processed in parallel because the distributed RAM is used. At the end of processing (reading operation, processing operation and writing operation), the signal of each color (finish_r, finish_g and finish_b) will be set to logic one. This means 42.5 clk was required as shown in Fig (2) with initial clk forced to be 1ms.

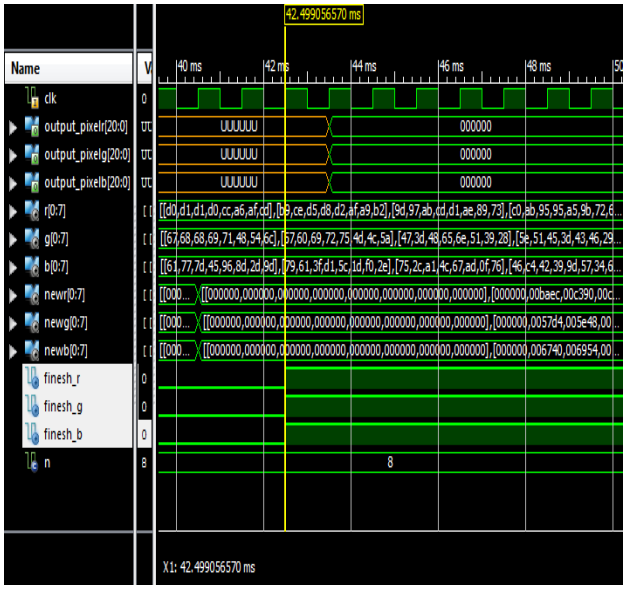


Figure 2. The Timing Diagram of ISim Simulator Using Spartan 6 and Virtex 5.

From the results presented in Fig. 6, it is clear that in the case of Spartan 6E, the total frequency is equal to 200 MHz, the maximum frequency is 71.18 MHz and the total number of occupied slices is 31 %. Furthermore, the processing time of the sampled RGB image (Ts) is 0.597 µs (42.5 clk) and the processing time of each pixel (T_p) is 5.53 ns ((42.5x0.597 µs)/(36x3)) as illustrated in Fig (2). At this moment, the three finishing signals are set to logic one at 42.5 ms. However, when the size of suspected RGB image file is 256x256 pixel, the number of frames per second F that wanted to be filtered, has been found to be 920 frames per second. This suggests that the maximum size of suspected RGB image file that making the filtered frames equals to 30 frames per second is 1417x1417 pixel, whereas the throughput of the stego filter component is 1380 Mbps and the speedup is 15045 times. In the case of Virtex 5, the total frequency is 100 MHz and the maximum operating frequencies is 81.55 MHz. Thus, the utilization summary for Virtex 5 is different from Spartan 6E.

The results in Table III show the comparison between utilization summary of the two used models of FPGA technology. In these tests, the filtering performed when the suspected image files corrupted by LSB and DCT steganography, respectively, and the secret stego content entirely destructed have been achieved. It is clear from the results that;

i. Repetition code 5 approach enhances the invisible watermarking robustness.

ii. Steganography insertion of sensed information causes minor alterations in the cover image file where the quality degrades. Therefore, steganography content acts as noise in the cover image file.

iii. The real time implementation of image processing or firewall requirements achieved by the two models of FPGA, Spartan 6 and Virtex 5. The invisible watermarking is necessary for achieving authentication as a result; authentication directory for licensed to protect it from destroying or disabling.

TABLE III . COMPARISON BETWEEN DEVICE UTILIZATION SUMMARY OF SPARTAN 6 AND VIRTEX 5.

Device Utilization Summary	*FPGA Model*	
	Spartan 6	*Virtex 5*
No. of CLK	42.5	42.5
Total Frequency (MHz)	200	100
Maximum Operation Frequency (MHz)	71.18	81.55
Processing Time of Each Pixel T_P (ns)	5.53	4.82
Processing Time of Sampled Image T_S (µs)	0.5970	0.5211
No. of Frame (256x256) /s	920	982
Max Size of Frame (PixelxPixel)	1417x1417	1517x1517
Percent of Occupied Slices (%)	31	19
Throughput (Mbps)	1380	1581
Speedup (Times)	15045	17237

6. CONCLUSIONS

The main scope of the research is to destroy the hidden stego content while keeping the carrier image file safe. The research presented two problems facing the adoption of such firewall, watermarking safe passage and the real time implementation of such system using FPGA technology. The research results verify these requirements and reached the following conclusions;

- Invisible watermarking forms exactly the same threats as that of steganography because it's a subset of steganography. Furthermore, repetition code 5 also fails in making the invisible watermarked files pass successfully. Therefore, the process of bypassing is adopted only for licensed users using authentication directory. This will allow the licensed invisible watermarked files to pass successfully with its secret content over the proposed firewall system.
- With visible watermarking, the system performs very well because it's a subset of cover file.
- Denoising approach is very attractive to destroy stego content entirely since the quality of the cover image enhanced because of their possibility to remove various noises from image files if exist including stego noise. For this reason, reverse steganography algorithm cannot retrieve secret message from the stego image files.
- Encrypted and virused (cookie) files have noisy manner as stego files and can be filtered by denoising approach. For this reason, the proposed firewall system can be a novel antivirus.
- The real time implementation achieved using various chips of FPGA technology such as Spartan 6 and Virtex 5 where the image processing speed, maximum frequency, throughput and speed up are very high. However, Virtex 5 is the best.
- This real time firewall installed on large networks or local ISP providers such as ministry, university, and county to protect them from any terrorist and malicious groups that benefited from Internet environment.

REFERENCES

[1] M. Bogdanoski, A. Risteski, S. Pejosk, "Steganalysis – a Way Forward Against Cyber Terrorism", IEEE Proceedings of 20th Telecommunication Forum, Belgrade, Serbia, November 2012.

[2] R. Goel, M. Garuba, Ch. Liu, "The Security Threat Posed by Steganographic Content on the Internet", IEEE Proceedings of International Conference on Information Technology, Las Vegas, USA, April 2007.

[3] F. Al-Naima, S. Ameen, A. Al-Saad, "Destroying Steganography Content in Image Files", IEEE Proceedings of Fifth International Symposium on Communication Systems, Networks and Digital Signal Processing, University of Patras, Patras, Greece, July 2006

[4] W. Jamieson, "Destruction of Steganography: Targeting the Least Significant Bit in 24 bit Images", University of Eastern Michigan, USA, 2007.

[5] R. Nivedhitha, S. Abirami,, K. Bala, and N. Raajan "Proficient Toning Mechanism for Firewall Policy Assessment", IEEE Proceedings of International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, India, March 2015

[6] Z. Trabelsi and V. Molvizadah, "Edu-Firewall Device: An Advanced Firewall Hardware Device for Information Security Education", IEEE Proceedings of 13th Annual Consumer Communications & Networking Conference (CCNC), 2016, 1, pp. 978-979

[7] L. Zhang, and M. Huang, "A Firewall Rules Optimized Model Based On Service-Grouping", IEEE Proceedings of 12th Web Information System and Application Conference (WISA), Jinan, China, September 2015.

[8] Th. Chomsiri, X. He, P. Nanda, and Z. Tan,:"Hybrid Tree-rule Firewall for High Speed Data Transmission", IEEE Transactions on Cloud Computing, 2016, PP, pp. 1-13

[9] I. Moskowitz,P. Lafferty, and F. Ahmed "Stego Scrubbing A New Direction for Image Steganography", IEEE Proceedings of Information Assurance and Security Workshop (IAW), West Point, New York, USA, June 2007.

[10] M. Al Terki, "Implementation and Evaluation of Stego Image Destruction Method", M.Sc. Thesis, Gulf University, Bahrain, January 2012

[11] S. Ameen and M. Al-Badrany, "Optimal Image Steganography Content Destruction Techniques", Proceedings of the International Conference on Systems, Control, Signal Processing and Informatics, Rhodes (Rodos) Island, Greece, July 16-19, 2013

[12] N. Le, Th. Le, and Y. Jang, "Optical Camera Communications Based Invisible Watermarking Technique", IEEE, Proceedings of International Conference on Information Networking (ICOIN), Kota Kinabalu, malaysia, January 2016

[13] A. Abdelhakim, H. Saleh. and A. Nassar, "Quality Metric-Based Fitness Function for Robust Watermarking Optimisation with Bees Algorithm", The Institution of Engineering and Technology (IET) Image Processing, 2016, 10, , pp. 247-252

[14] V. Singh, P. Dahiya, and S. Singh, "Smart Card Based Password Authentication and User Anonymity Scheme using ECC and Steganography", IEEE Proceedings of International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, India, September 2014

[15] K. Thamizhchelvy and G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm", IEEE Proceedings of International Conference on Computing Sciences (ICCS), Phagwara, India, September 2014

[16] A. Ibrahim, P. Gastaldo, H. Chible and M. Valle "Real-Time Digital Signal Processing Based on FPGAs for Electronic Skin Implementation", Sebsors, 17, 558; doi:10.3390/s17030558

[17] N. Devineni and I. Panahi, "Analysis and Real Time Implementation of 2-Channel Adaptive Speech Enhancement Using Labview FPGA", IEEE, Proceedings of International Conference on Electro/Information Technology (EIT), Mankato, USA, May 2011

[18] T. Kondo, R. Kitaoka, and W. Chujo, "Multiple-Access Capability of LED Visible Light Communication With Low-frame-rate CMOS Camera for Control and Data Transmission of Mobile Objects', IEEE, Proceedings of International Symposium on System Integration, Nagoya, Jaban, december 2015.

[19] Rohith, S., Hari bhat, K.: 'A Simple Robust Digital Image Watermarking against Salt and Pepper Noise using Repetition Codes', International Journal on Signal & Image Processing (IJSIP), 2012, 3, pp. 47-54

[20] I. Kaur, L. Rohilla, A. Nagpal, B. Pandey, and S. Sharma, "Different Configuration of Low-Power Memory Design Using Capacitance Scaling on 28-nm Field-Programmable Gate Array. In System and Architecture" Springer: New York, NY, USA, 2018; pp. 151–161.

Muthana R. Al-Sultan received BSc in Electrical and Electronics Engineering in 2008 from University of Mosul, Mosul. Next, he has been awarded the degree of M.Sc. degree in Computers Networks & Communications Engineering in 2015 from University of Mosul, Mosul**.** From 2010 till now, he worked as an electrical engineer in engineering affairs at University of Baghdad while from 2015 till now he worked as an assistant lecturer in the College of Engineering, University of Baghdad for two materials (Physics & Engineering Analyses lecturer).

Siddeeq Y. Ameen Professor of data communication and processing and MIEEE with FHEA. He received BSc in Electrical and Electronics Engineering in 1983 from University of Technology, Baghdad. Next awarded the MSc and PhD degree from Loughborough University, UK, respectively in 1986 and 1990 in the field of Digital Communication Systems and Data Communication. From 1990- 2006, Professor Siddeeq worked with the University of Technology in Baghdad with participation in most of Baghdad's universities. From Feb. 2006 to July 2011 he was a Dean of Engineering College at the Gulf University in Bahrain. From Oct. 2011-Sep. 2015 he joined University of Mosul, College of Electronic Engineering as a Professor of Data Communication and next Dean of Research and Graduate

Studies at Applied Science University, Bahrain till Sep. 2017. Presently, he is quality assurance advisor at Duhok Polytechnic University, Duhok, Iraq. Through his academic experience, he published over 100 papers and a patent in the field of data communication, computer networking and information security and supervised over 110 PhD and MSc students. He won the first and second best research in Information Security by the Arab Universities Association in 2003.

Wafaa Mustafa Abduallah received Ph.D at 2015 in Computer Science from IIUM, Malaysia and the M.Sc. in Computer Science in 2010 from University of Duhok, Iraq. She received B.Sc. in Computer Science in 2005 from Mosul University. She is currently working as lecturer at the College of Computers and IT, Nawroz University, Duhok, Iraq.