International Journal of Cyber Security and Digital Forensics

(IJCSDF)
ISSN 2305-0012

Volume 5, Issue 1
2016

SDIWC
www.sdiwc.net

ISSN: 2305-0012 (online)

International Journal of
Cyber-Security and Digital Forensics

2016

Overview

The International Journal of Cyber-Security and Digital Forensics (IJCSDF) is a knowledge resource for practitioners, scientists, and researchers among others working in various fields of Cyber Security, Privacy, Trust, Digital Forensics, Hacking, and Cyber Warfare. We welcome original contributions as high quality technical papers (full and short) describing original unpublished results of theoretical, empirical, conceptual or experimental research. All submitted papers will be peer-reviewed by members of the editorial board and selected reviewers and those accepted will be published in the next volume of the journal.

As one of the most important aims of this journal is to increase the usage and impact of knowledge as well as increasing the visibility and ease of use of scientific materials, IJCSDF does NOT CHARGE authors for any publication fee for online publishing of their materials in the journal and does NOT CHARGE readers or their institutions for accessing to the published materials!

Publisher

The Society of Digital Information and Wireless Communications
Miramar Tower, 13 Nathan Road, Tsim Sha Tsui, Kowloon, Hong Kong

Further Information

Website: http://sdiwc.net/ijcsdf, Email: jcs@sdiwc.net,
Tel.: (202)-657-4603 - Inside USA; 001(202)-657-4603 - Outside USA.

The issue date is January 2016.

ISSN: 2305-0012 (online)

International Journal of
Cyber-Security and Digital Forensics

2016

Volume 5, Issue 1

CONTENTS

ORIGINAL ARTICLES

ISSN: 2305-0012 (online)

International Journal of
Cyber-Security and Digital Forensics

2016

A Note of Appreciation to Dr. Ali Dehghantanha - An Imminently Qualified and Outstanding Researcher in Cyber Security and the founder and the first editor in chief of "International Journal of Cyber Security and Digital Forensics"

Professionals such as Dr. Ali Dehghantanha are a credit to cyber security and digital forensics research community and an influencer to developments in the field. Dr. Ali has a long history of serving in different professional and academic societies resulted to many contributions in the field. His significant research track in different domains of cyber security is an evident of his expertise. He has published more than 100 scientific publications and he is among the most cited scholars in the field. He has led development of two Linux-distros namely “Malux: A Malware Anlaysing Linux” and “Limund: A Security Toolbox for Cyber Physical Systems (CPS)” ; the latter is still the only available Linux specifically designed for security researchers in Internet of Things. Moreover, his profound contributions to "privacy respecting digital investigation" cross-disciplinary field of research put him among the very few experts in the field and brought him a Marie Curie International Incoming Research Fellowship award. The Marie Curie Fellowships are Europe’s most competitive and prestigious awards, and are aimed at fostering interdisciplinary research and international collaborations. Beyond research, the educational system he has developed for teaching cyber offensive techniques to students is adopted by many schools and universities in all around the globe which awarded a Gold medal for him in Malaysia Trade Exhibition 2013.

Dr. Ali has served as the editor in chief for International Journal of Cyber Security and Digital Forensics (IJCSDF) since its establishment in 2012. Under his leadership the journal was indexed in more than 20 different academic indexing services and published more than 60 high quality research papers. His decision in Jan 2016 to appoint a new editor in chief for the journal was not taken lightly. Although he would still serve as an advisor for the journal as necessary but his decision was respected. Both IJCSDF editorial board and its publisher the "Society of Digital Information and Wireless Communications" would like to further their sincere thanks to his efforts and wish him the best in future.

Chief Editors

Lei Xu, University of Houston, United States
Dragan Perakovic, University of Zagreb, Croatia

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(1): 1-9
The Society of Digital Information and Wireless Communications, 2016 (ISSN: 2305-0012)

The Role of the Refrigerator in Identity Crime?

Eric Holm
Federation University Australia
P.O. Box 668, Mount Helen 3353
e.holm@federation.edu.au

ABSTRACT

This paper explores how botnets in smart devices are exacerbating identity crime. This paper places the refrigerator at the heart of this discussion of the Internet of things that has become connected through the Internet and thereby susceptible to botnets and the collection of personal identification information as an enabler for identity crime. The paper highlights the fallibility of these devices and provides some mechanism to deal with these new risks and presents discussion on the need to for this relationship to be further explored.

KEYWORDS

Botnet, computer crime, identity crime, identity theft, Zeus botnet.

1 INTRODUCTION

Botnets are connected computers communicating across the Internet to complete various tasks and have become common in many acts including having become known through their association with denial-of-service attacks [1] and with the distribution of spam [2]. To commit these types of actions, botnets remain concealed in a victim's computer and take commands from their master while stealthily spreading themselves across the Internet [3]. The term 'botnet' is an amalgam of two words, namely the 'robot' and the 'network' [4]. The robotic feature of the program relates to the autonomous nature of the software and the network and the pathway for them to be disseminated [4]. The use of botnets has expanded to incorporate many crimes and the criminality surrounding them is evolving [5].

Not all botnets are bad botnets; for instance good botnets are used by search engine providers such as Google to improve their search engines [3]. These improvements are positive for end users and certainly enhance the ways in which the Internet is used [3]. However, at the same time, botnets are widely known for inflicting harm through their potential for use in activities, some of which are criminal [1], [2]. What makes botnets dynamic is their ability to be customized by programmers for a variety of purposes that can include both criminal and non-criminal acts. For this reason, they can inflict widespread damage through criminal acts, particularly as they can spread themselves across the Internet. In this way, they have become recognized as a pandemic to the security of the Internet [6]. The Zeus botnet is an example of a widely known botnet that is used for stealing individual and corporate credentials [7]. The Zeus toolkit has historically infected millions of computers in the United States and worldwide [8].

2 WHAT DOES THE BOTNET DO?

The primary role of the botnet is to function according to the programmed instructions it obtains, and to report back to the bot-master (the person in charge of the botnet) [9]. The master of the botnet provides commands that direct the many actions of the botnet. In following these instructions, the botnet will routinely check with the master for new commands [10]. The programming of commands from the bot-master thus define the scope of criminal activities undertaken. The control is understood to entail 'command and control' which is a phrase used to express the dual function of the bot-master in controlling the botnet in the way desired while also adapting this control as desired through

command [9]. The overwhelming strength of a botnet attack comes from the coordination of computers co-opted for the purpose and as the number of computers increases, the army becomes larger and the associated threats to the controlled computers increase [9]. Through this process, the botnet aims to remain concealed within devices connected on the Internet to avoid detection [11] and accepts these instructions to operate in ways that are remote and also cover which support the primary role of the botnet [12].

The adaptability of botnets makes it possible to configure their use for identity crime; the impetus for this activity is about using the botnet for the collection of personal information as the catalyst to committing identity crime [12]. Under Australian criminal law, unauthorized dealing with personal identification information is a key aspect of identity crime [13]. Central to the crime is the possession of and dealing with personal identification information which includes people's dates of birth and their full names and addresses, but is not limited to these [13]. For the crime to apply, this information must be used or dealt with [13]. In this way, information has value when considered according to its propensity for misuse [14]. Accordingly, the value of this information depends on what can be done with it, but the mere possession of such information is regarded as an offense, for instance under the Australian Commonwealth Criminal Code [13].

Botnets can be created with a relatively low level of technological skill and the skill utilized to develop these will vary according to the skills of the person creating them [15]. Consequently, the broader market for criminal "services" online, to be used for cyber-crimes, also continues to grow [15]. For instance, services to develop botnets are becoming more prominent as is the provision of botnets to order, such as for the purposes of denial-of-service attacks or to spam [16]. The level of sophistication of the botnet varies as does the level of obfuscation based on their design and implementation [6]. As a consequence, the market for the development of services supporting the development of criminal services is increasing as is the level of sophistication generally.

One aspect of botnets that differentiates their creation from other acts is that they are relatively inexpensive to create and manage for a variety of purposes whether legal or not. They are often sold as customizable toolkits, and in this way, the customization provides for adaptability [17]. Starting from a base line of a Zeus botnet, the adaptation of botnets serves a number of functions, including the collection of personal identification information and tracking online behavior patterns [18]. The botnet can readily be adapted for undertaking a variety of actions including those that could be used to facilitate identity crime [19]. A consequence of this is that botnet activity might result in myriad criminal offenses linked to identity crime as well as other crimes [8]. The Australian Institute of Criminology has identified that botnets play a significant role in the promulgation in phishing attacks and their adaptability makes them into a tool of crime [20]. Compounding these features is the pervasive nature of botnets and the ability to use them to facilitate coordinated mass attacks across the Internet [21]. The botnet army obtains strength from its size and scale, and it can be enormous [21]. In this respect, the pervasive nature of the crime coupled with the customization of the botnet is what makes this tool unique if used for crime [8].

The refrigerator has been used in this article to illustrate how an innocuous device, namely the household refrigerator, can be used to perpetrate offenses relevant to identity crime through botnets. The refrigerator can only be used for the distribution of botnets if it is 'smart' and what makes a device 'smart' is its web enabled interoperability [22]. Increasingly, domestic household appliances have Internet connectivity and thereby have progressively become 'smart' and consequently potential targets of botnet attacks [23]. 'Smart' devices include tablets, computer routers and switches, among others [24]. The attractiveness of these devices as targets for botnets stems from the extraordinary number of devices connected to the Internet [24] and the technological security weaknesses these devices have [24]. Mobile smart devices tend to have

infrequent updates and lackluster security measures [25]. Smartphones for instance, have become vulnerable to botnet attacks for many of these reasons [26]. Eslahi, Salleh and Anuar have referred to these botnets as MoBots as they operate through mobile devices and through the use of mobile networks [25]. Damballa Research Laboratory in 2011 indicated that up to 40,000 infected computer systems were detected within the first six months of that year [27]. These devices add to the bulk of compromised systems and potential armies that can be involved with botnet activity. Accordingly, these contribute toward the spread of risks associated with botnets and their related crimes [28].

The phrase 'Internet of things' is used to explain how so many devices or 'things' are interoperable with the internet [12]. The Internet of things expresses the interconnection on the Internet of everyday objects including those mentioned that share this space [12], [29]. These devices share an affinity through the extent they interoperate on the Internet but also by the ways they could contribute to the armies of remote controlled computers connected to the Internet. In this way, the innocuous kitchen device, the 'smart refrigerator' can now play a clandestine role in perpetuating identity crime. On the vulnerability of these devices on the Internet of things, Hewlett-Packard suggests that around 70 per cent of devices connected to the Internet have vulnerabilities [30]. This means that a significant number of devices could play a role in botnet distribution. The most notable problems for many of these devices is the lack of encryption, the ease of access, and the absence of security measures such as the use of passwords which facilitate their use in this way [30]. Furthermore, a problem with these devices is that there is no easy way to install an antivirus or related security mechanism, which also applies to most refrigerators [30].

3 EXAMPLES OF BOTNETS

An example involving a refrigerator, television and home router being used in a botnet attack in Australia occurred in 2014; they were found to have sent 750 thousand malicious emails [31]. However, a number of other examples of botnet attacks have been known to have a far more profound impact. A key example of a major botnet attack in Australia was the Citadel, a botnet that targeted banking credentials and this was responsible for losses amounting to the equivalent of more than US$100 million [32]. The Citadel botnet attack identified where financial information was entered by a computer user and would then extract that information for the purposes of committing fraud [33]. The impact of this crime was profound in Australia, with over 30,000 detected instances of infected computers infected in Sydney alone. The overall losses attributed to this botnet alone have been estimated at over A$500 million dollars [33]. The Gameover Zeus botnet similarly compromised over 75,000 computers and compromised more than 2,500 international organizations [34]. The efforts to disrupt this botnet were only possible due to a multinational effort that took place to investigate offenders [35]. The Federal Bureau of Investigation suggested that this botnet attack was one of the more significant attacks of its type that they have investigated, due to the worldwide infestation [32], [34]. Indeed, the harm caused by botnet attacks is difficult to measure based on their size in isolation, but harm can be measured by considering both the respective size and reach of a botnet. For example, by using a botnet comprised of 183,000 zombie devices, criminals harvested 310,000 items of identity including 310,000 bank account details, credit card details as well as social networking credentials [36].

4 CAN THE REFRIGERATOR BE USED FOR IDENTITY CRIME?

The refrigerator itself cannot be a criminal; for the purposes of identity crime a refrigerator is not a natural person and cannot possess the 'intent' to commit a crime [37]. Likewise, it is difficult to assert that the botnet is the criminal as similarly it cannot possess that intention to commit a crime. Rather, the refrigerator can be an instrument of crime under certain circumstances. In this regard, the refrigerator is a resource that can be used to facilitate a crime, but it is dependent on the intentions of the criminal. Symantec provides an

example of this where a criminal used a refrigerator to send 100,000 spam through an installed botnet [38]. Hence, rather than the refrigerator or the bot being the criminal, it is the person in control of the botnet that has the criminal intent. To perpetrate the crime, the refrigerator and the botnet are used together to enable identity crime.

Identity crime is defined by the Organisation for Economic Co-operation and Development (OECD) as a crime where one party uses the personal information of a person in an unlawful manner [39]. Key to establishing an identity crime is to establish the possession of or use of personal identification information [13]. Within the literature, a distinction has been drawn between identity theft and fraud, to delineate cases in which the theft involves only the theft of identification information and where it involves fraud [40]. This is despite the fact that one action, the theft of information, is often the catalyst for the other, the fraud associated with the theft. Common to any allegation of identity crime is the unlawful use of stolen information, typically with the view to obtaining some advantage which might relate to fraud, but does not always need to [40]. The European Network and Information Security Agency similarly suggests that common to the perpetration of cybercrimes is the desire to extract credentials for some gain [41].

In relation to specific crimes pertaining to this, identity theft is an offense if one's identity is obtained and is possessed wrongfully [42]. As discussed, the criminal offense is the unlawful use of another's personal information [43], and many concede this as the basis for the establishment of their crime. It should be noted that Australian states and territories construe the laws relating to this crime slightly differently from each other, and there are considerable variations in the punishments associated with committing these offenses. Penalties vary from five years' imprisonment upon conviction, but up to ten years' imprisonment is possible in some states / territories [44]. Similar contrasts can be made between the penalties for offenses when comparing Australia and other countries, most notably the United States [45]. Furthermore, whereas identity crime is recognized as a crime in most Australian localities, in some countries it is not thus recognized in all, and this results in disparities with respect to offenses and penalties. This disparity challenges the consistency of offense penalties applied, but this discussion falls outside the scope of this paper.

In Australia, the use of a botnets to facilitate crime is covered by criminal offenses that include those relating to access [46], interference [47], and misuse of devices [48]. These are offenses that symbolize the nature of undesired and undesirable behavior. The punishment commensurate with the crime(s) is often determined by considering the offenses committed. For the purposes of this paper, assuming the requisite elements of the unauthorized modification of data are satisfied, then this can have a penalty of up to 10 years' imprisonment [47]. Likewise, the offense of the unauthorized impairment of electronic communication carries similar penalties [49]. Further, if a botnet is involved with the dissemination of spam and phishing this will attract different or further sanctions [50] and this is plausible as a relationship can exist between spam and phishing. Indeed, if this crime is directly linked to that of identity crime, then in absence of aggravated provisions, the compounding penalties of the offenses listed would apply.

5 INDICATORS OF THE CRIME

Many users remain unaware of the presence of botnets on their devices [3]. There can be difficulties in detecting botnet activity, particularly when they are designed to remain concealed. Further, the evolution of different platforms has increased the difficulties of detecting the warning signs that a botnet is present [51]. Another challenge in the detection of botnet attacks is that botnets reside differently depending on their customization and dissemination [25]. The determination of location is particularly challenging for mobile devices as they can be used anywhere [52]. Having stated these difficulties, the United States Federal Bureau of Investigation states that there are a number of indicators that make it evident that a computer has been infected

by botnets [35]. Common warning signs include system slow-downs related to high levels of disk activity [35], [3]. However, the indicators of identity theft are far more difficult to identify. Interestingly, governmental bodies in the United States remain well placed to provide commentary on identity crimes, particularly as they remain prominent and public there. The United States Federal Trade Commission proclaimed in 2013 that identity theft was the most common national consumer complaint [53].

In responding to this crime, there are often delays in its detection by victims, and this complicates the information known about the crime [11]. Investigation can be hampered by the time lapse between the identity crime occurring, and its being reported [53]. Because of this delay, the perpetrators have ample opportunity to avoid apprehension [36]. Law enforcement agencies are similarly impeded due to the geographic dispersion of these crimes particularly where the identity crime has a relationship with botnets [54]. The Internet provides many criminals with anonymity and the jurisdictional problems faced with the geographic reach of these crimes impact on the ability of law enforcement agencies to respond [55]. Delays in detecting the crime adds to the complexity of responding to the crime [56] and complicate the ability of law enforcement agencies to deal with the crime in a timely manner [57]. Identity crime itself can be a crime that can be difficult to detect [58] and a part of this problem is that mostly the crime is eventually detected by the individual, but not usually until the individual detects unauthorized transactions [59]. The botnet is designed to be elusive and due to this characteristic, it too makes the detection and responses to it difficult.

6 THE NEED FOR DATA AND RESPONSES

Information can be a barrier to understanding crime and this exists for many cybercrimes [60]. While there are bodies that are well placed to collect information relevant to these crimes, often the data relevant to crimes are construed narrowly and certainly seldom shared [57]. The sharing of knowledge related to these types of emerging crimes needs to be improved so that this crime and others like it can be better understood [42]. In addition, a repository of information related to the crime will invariably assist all relevant stakeholders in understanding the prevailing risks from this crime [42]. In this regard, governments can play a role in collecting data in relation to this crime as they can also play a role in disseminating data relevant to it.

Governments play a key role in the responses to crime as they can ensure coordinated efforts are made through relevant stakeholders and constituents. These crime control measures are needed so that governments, international bodies, ISPs as well as other stakeholders work together as they are all impacted in some way by these crimes [61]. The coordination imperative is complicated by the many different agendas that exist for each of these parties [61]. In this regard, there are barriers to achieving this, namely around sovereignty but also by competing agendas [61]. Nevertheless governments play an important role in dealing with the development of strategic and policy responses to these emerging crimes which are critical to influencing regulatory responses as well as other responses [62]. In particular, there is a need for better coordination between government and industry in relation to responses to these crimes [63]. It is hoped that a greater awareness of the risks associated with these newly emerging variants of crime will prompt the actions of government needed to deal with these crimes.

Regulatory responses to crime need to be better defined to match the risks that the crime presents. In the absence of data on this, responses can be difficult. There can be some difficulties in capturing new offense variations such as those discussed here, due to the ways that legislation is currently constructed. Whereas regulatory responses can be drafted narrowly, they can fail to capture the desired criminal behaviors as they are applied intently. Alternatively, they might be drafted broadly and consequently become diluted, which is problematic as they then fail to be specific enough to capture the criminal activities intended [64]. The difficulty in calibrating appropriate regulatory responses is to find a

balance between regulations that are tight enough to capture the necessary variations of offenses, but loose enough to deal with the varieties of crime. Beyond the original drafting of legislation relating to these offenses, the responses to crime need to have some flexibility to adapt to newly emerging variations of offending. It is for this reason that the regulatory responses have be adaptable to encompass the challenges presented by these crimes [57]. At present, this remains problematic as the offending associated with identity crime and botnets has no universally accepted offense or definition. Whereas this requires some dynamism in the application of criminal sanctions for related offenses, it also presents motivations for the laws to be further developed.

Any response to this crime will also require a collaborative international effort due the crime's multi-jurisdictional nature [41]. A necessary precursor to dealing with these problems is the harmonization of laws related to the crimes at an international level [41]. Within the international mechanisms that promote harmonization of cybercrimes, there is little coverage of identity crime and botnets [65]. Having said that, it would be plausible for these offenses to be subsumed or captured within related offenses. Further, a positive benefit of international agreements relating to cybercrime is that they foster the development of domestic responses to related offenses [60]. However, more development of the law, particularly to facilitate harmonization, is needed for crimes that straddle jurisdictional boundaries and offense types.

A better understanding of the relationship between individuals and technology vulnerabilities would also increase the stringency of responses. Behavioral factors are multifaceted and need to be better understood particularly as humans remain (in a general sense) a known weakness in cyber security [26]. This weakness has relevance to both botnets and identity crime insofar as these crimes are linked together often by the fallibility of human behavior. Despite many of these already having been investigated, a further insight into these in the specific context of identity crime and botnets will fuel the development of preventative steps needed to address the risks by focusing on the behavioral problems [62]. However, at the same time, there is an arms race between those that wish to protect information and those that are looking to exploit it [55]. Nonetheless, as the techniques to deal with bots and identity crime from a behavioral perspective evolve, so do the many ways of working around technological solutions to prevent these risks [2]. For this reason, it is important that the preventative steps supersede the actual risks.

Technological responses to crimes also provide for ways of dealing with crime through non regulatory means. Technological responses provide another way of understanding how these crimes can be responded to, with measures such as filtering, blocking and blacklisting as select example of ways of preventing such attacks from taking place [41]. Technological responses like encryption and authentication also provide for ways of preventing identity crime, although the direct relationship between these preventatives and the crime are not definitive [57]. Indeed, some technological responses operate to complement regulatory and other responses but because these crimes are both pervasive and adaptable, the responses to this crime also need to be dynamic [61]. Indeed, as methods to perpetrate identity crime emerge, so do the technological methods that overcome them and for this reason an increased focus on the development of technological responses is needed. Whereas technological responses to any cybercrime are not a panacea to resolving this type of crime, they provide ways of dealing with the crime in ways other than regulation [41]. These responses to crime can play an important role in reducing the incidence of botnet attacks as well as identity theft [42]. In respect to the adoption of approaches other than regulation, the benefit of multiple approaches to dealing with crime is that broader policy objectives underpinning their existence can be met [39].

7 DISCUSSION AND CONCLUSION

The emergence of smart devices has contributed to the Internet of things which represents a conglomeration of devices connected to the

Internet. These devices, which include the smart refrigerator, provide mechanisms through which botnets can operate and if appropriately customized, can gather the information needed for identity crimes to be perpetrated. In this way, this paper has deliberated on how the botnet could have a positive impact on the occurrence of identity crime through these types of smart devices. The paper places the refrigerator at the heart of the discussion as a smart device that plays a role in botnet attacks, using this smart device as an exemplar to highlight how the botnet could be infiltrating this innocuous device due to their lackluster preventative measures.

The paper explored responses to botnets and identity crime and presented a discussion about the challenges of operationalizing these. The paper contends that whereas these crimes are considered separately from one another, the relationships between them have only rarely been considered. Lastly, the paper provides some options for dealing better with identity crime and underpinning these is the need for more research to be undertaken to understand how botnets share relationships with crimes like identity crime.

8 REFERENCES

1. C. Elliott, "Botnets: to what extent are they a threat to information security?," *Information Security Technical Report*, vol. 14, no. 3 Aug, pp. 79-83. Feb. 2011.
2. R. Rahman, "Legal jurisdiction over malware-related crimes: from theories of jurisdiction to solid practical application," *Computer Law and Security Review*, vol. 28, no. 4, pp. 403-415. Aug. 2012.
3. J. Gavel, "Examining the criminology of bot zoo," in *International Conference on Information*., Singapore, 2007, pp. 1-6.
4. Kaspersky. (2015). "What is a botnet?," [Online]. Available: http://www.kaspersky.com/au/internet-security-center/threats/botnet-attacks. [Accessed: Feb. 13, 2015].
5. Symantec. (2009). Bots & Cybercrime [Online]. Available: http://www.symantec.com/norton/theme.jsp?themeid=botnet. [Accessed: Feb. 13, 2015].
6. A. Al-Bataineh, and G. White, "Analysis and Detection of Malicious Data Exfiltration in Web Traffic," in *International Conference on Malicious and Unwanted Software*., Puerto Rico, 2012, pp. 16-18.
7. D. Andriesse, C. Rossow, B. Stone-Gross, D. Plohmann, and H. Box, "Highly Resilient Peer-to-Peer Botnets Are Here: An Analysis of Game over Zeus," in *International Conference on Malicious and Unwanted Software: "The Americas*., Puerto Rico, 2013, pp. 116-123.
8. H. Binsalleeh, T. Ormerod, T, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi, and L. Wang, "On the analysis of the Zeus Botnet crimeware toolkit," in *International Conference on Privacy Security and Trust*.,Ottawa, 2010, pp. 31-38.
9. M.T. Banday, J.A. Qadri, and N.A. Shah, "Study of Botnets and Their Threats to Internet Security," [Online]. Available: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1278&context=sprouts_all. [Accessed: Feb 6, 2015].
10. C. A. Schiller, J. Binkley, G. Evron, C. Willems, T. Bradley, D. Harley, and M. Gross, *Botnets: The Killer Web App*. USA: Syngress. 2007, pp. 19.
11. A.K. Sood, R.J. Enbody, and R. Bansal. (2013, Feb.). Dissecting SpyEye – Understanding the design of third generation botnets. *Computer Networks* [Online]. 57 (2), pp. 436-450. Available: http://www.sciencedirect.com/science/article/pii/S1389128612002666
12. F. Xia, L.T. Tang, L. Wang, A. and A. Vinnel, "Internet of Things," *International Journal of Commercial Systems*, vol. 25, no. 9, pp. 1101-1102, Sep. 2012.
13. Commonwealth Criminal Code Act 1995 (Cth), Division 372.
14. E. Holm, and G. Mackenzie, "The importance of mandatory data breach notification to identity crime," in *Cyber Security, Cyber Warfare and Digital Forensic.*, Lebanon, 2014, pp. 6-11.
15. S. Gallagher, "A beginner's guide to building botnets-with little assembly required," *Ars Technica*. [Online]. Available: http://arstechnica.com/security/2013/04/11/a-beginners-guide-to-building-botnets-with-little-assembly-required/. [Accessed: Apr. 17, 2015].
16. D. Manky, "Cybercrime as a service: a very modern business," *Computer Fraud & Security*, no. 6, pp. 9-13, Jun. 2013.
17. A. Mohaisen, and O. Alrawi, "Unveiling Zeus: automated classification of malware samples," in the *International Conference on World Wide Web Companion*., Reston, VA, 2013, pp. 829-832.
18. Australian Institute of Criminology, "More Malware: Adware, Spyware, Spam and Spim. Australian Institute of Criminology," Canberra, Australia. [Online]. Available: http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb011.aspx. [Accessed: Feb. 13, 2015].
19. G.P. Schaffer, "Worms and viruses and botnets, oh my!: Rational responses to emerging Internet threats," *IEEE Security & Privacy*, vol. 4, no. 3, pp. 52-58. May, 2006.
20. Australian Institute of Criminology, "*Zombies and botnets*," [Online]. Available: http://www.aic.gov.au/publications/current%20series/tandi/321-340/tandi333.html. [Accessed: Feb. 13, 2015].

21. R. Siciliano, "Botnets lead to identity theft. McAfee," [Web log post]. Retrieved from McAfee. [Online]. Available: http://blogs.mcafee.com/consumer/identity-protection/botnets-lead-to-identity-theft. [Accessed: Apr. 17, 2015].
22. Networkworld, "*Can TVs and refrigerators really spew botnet spam?"* [Online]. Available: http://www.networkworld.com/article/2173783/network-security/can-tvs-and-refrigerators-really-spew-botnet-spam-.htmlhttp://www.networkworld.com/article/2173783/network-security/can-tvs-and-refrigerators-really-spew-botnet-spam-.html. [Accessed: Feb. 26, 2015].
23. The Economist, "*Spam in the fridge,"* [Online]. Available: http://www.economist.com/news/science-and-technology/21594955-when-internet-things-misbehaves-spam-fridge. [Accessed: Apr. 17, 2015].
24. M. Kassner, "Internet of Things botnet may include TVs and a fridge," Tech Republic. [Online]. Available: http://www.techrepublic.com/blog/it-security/internet-of-things-botnet-may-include-tvs-and-a-fridge/. [Accessed: Feb. 26, 2015].
25. M. Eslahi, R. Salleh, and N.B. Anuar, "MoBots: A New Generation of Botnets on Mobile Devices and Networks." in *International Symposium on Computer Applications and Industrial Electronics*., Malaysia, 2012. – page 262-266.
26. N. MacEwan, "A Tricky Situation: Deception in Cyberspace," *Journal of Criminal Law*, vol. 77, no. 5, pp. 417-432. Oct. 2013.
27. Damballa Labs, "Threat Report," [Online]. Available: https://www.damballa.com/downloads/r_pubs/Damballa_Threat_Report-First_Half_2011.pdf. [Accessed: Apr. 25, 2015].
28. M. Postman, "iPhone Viruses: Ikee.b Worm," [Online]. Available: http://www.letsunlockiphone.com/ios-viruses-iphone-ikee-b-worm. [Accessed: Apr. 25, 2015].
29. D. Goodin, "Is your refrigerator really part of a massive spam-sending botnet?" Ars Technica. [Online]. Available: http://arstechnica.com/security/2014/01/is-your-refrigerator-really-part-of-a-massive-spam-sending-botnet/. [Accessed: Apr. 17, 2015].
30. C. Griffith, "Bitdefender sells antivirus for your fridge in a box," The Australian. [Online]. Available: http://www.theaustralian.com.au/business/technology/bitdefender-sells-antivirus-for-your-fridge-in-a-box/story-e6frgakx-1227239260188. [Accessed: Feb. 26, 2015].
31. The Age Newspaper, "Cyber-attack that sent 750k malicious emails traced to hacked refrigerator, TVs and home routers," The Age. [Online]. Available: http://www.theage.com.au/it-pro/security-it/cyber-attack-that-sent-750k-malicious-emails-traced-to-hacked-refrigerator- tvs-and-home-routers-20140120-hv96q.html. [Accessed: Feb. 11, 2015].
32. G. Gross, "Law enforcement agencies disrupt Gameover Zeus botnet," Goodgearguide. [Online]. Available: http://www.goodgearguide.com.au/article/546595/law_enforcement_agencies_disrupt_gameover_zeus_botnet/. [Accessed: Feb. 13, 2015].
33. L. Hopewell, "After the bust: how taking down one botnet killed 98 Per Cent of Australian Wire Fraud," Gizmodo. [Online]. Available: http://www.gizmodo.com.au/2014/06/after-the-bust-how-taking-down-one-botnet-killed-98-per-cent-of-australian-wire-fraud/. [Accessed: Feb. 13, 2015].
34. Calvert, "Beware the Kneber Botnet," [Online]. Available: http://www.calvert.net.au/2010/02/25/beware-the-kneber-botnet/. [Accessed: Feb. 13, 2015].
35. Federal Bureau of Investigation, "Gameover Zeus Botnet Disrupted," [Online]. Available: http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/gameover-zeus-botnet-disrupted. [Accessed: Feb. 13, 2015].
36. United Nations, "Comprehensive Study on Cybercrime," [Online]. Available: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. [Accessed: Apr. 25, 2015].
37. L. Sebba, "Crime Seriousness and criminal intent," *Crime & Delinquency*, vol. 30, no. 2, pp. 227-244. Apr. 1984.
38. BBC News, "Fridge sends spam emails as attack hits smart gadgets," [Online]. Available: http://www.bbc.co.uk/news/technology-25780908. [Accessed: Apr. 17, 2015].
39. Organisation for Economic Co-operation and Development, "Scoping Paper on Online Identity Theft," [Online]. Available: http://www.oecd.org/sti/40644196.pdf. [Accessed: Apr. 17, 2015].
40. G.R. Newman, "The problem of Identity Theft. Centre for Problem-Oriented Policing," [Online]. Available http://www.popcenter.org/problems/identity_theft/. [Accessed: Jan. 23, 2015].
41. D. Plohmann, E. Gerhards-Padalla and F. Leder, "Botnets: Detection, Measurement, Disinfection and Defence. European Network and Information Security Agency," [Online]. Available: http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport. [Accessed: Jan. 12, 2015].
42. European Commission, "Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft," [Online]. Available: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf. [Accessed: Apr. 25, 2015].
43. Commonwealth Criminal Code Act 1995 (Cth), Division 372.
44. Commonwealth Criminal Code Act 1995 (Cth), Division 372.1
45. 18. USC § 1028. (a)(7) (1998).

46. Commonwealth Criminal Code Act 1995 (Cth), Division 477, Section 477.1.
47. Commonwealth Criminal Code Act 1995 (Cth), Division 477, Section 477.2.
48. Commonwealth Criminal Code Act 1995 (Cth), Division 477, Section 478.3 and 478.4.
49. Commonwealth Criminal Code Act 1995 (Cth), Division 477, Section 477.3.
50. Spam Act 2003 (Cth) Section 5.
51. K. Bora, K, "Mobile malware increased by 700% Over 2011, Android No. 1 Targeted Platform: McAfee," International Business Times [Online]. Available: http://www.ibtimes.com/mobile-malware-increased-700-over-2011-android-no-1-targeted-platform-mcafee-779557. [Accessed: Apr. 25, 2015].
52. N. Leavitt, "Mobile Security: Finally a serious problem?," *Computer*, vol. 44, no. 6. pp. 11-14. Jun, 2011.
53. Federal Trade Commission, "FTC Announces top national consumer complaints for 2013," [Online]. Available: http://www.ftc.gov/news-events/press-releases/2014/02/ftc-announces-top-national-consumer-complaints-2013. [Accessed: Feb. 9, 2015].
54. Australian Institute of Criminology, "CRS Report for Congress - Botnets, cybercrime, and cyber terrorism: vulnerabilities and policy issues for congress," [Online]. Available: http://www.aic.gov.au/publications/current%20series/tandi/321-340/tandi333.html. [Accessed: Feb. 13, 2015].
55. M. Eriksen-Jensen, "Holding Back the Tidal Wave of Cybercrime," *Computer Fraud and Security*, vol.31, no. 3, pp. 10-16. Mar, 2013.
56. A. MacGibbon, "Australian e-Commerce Safety Guide. Government of South Australian," South Australia. [Online]. Available: http://www.cbs.sa.gov.au/assets/files/EcommGuide_2005.pdf. [Accessed: Apr. 17, 2015].
57. E. Holm, (2012, June). Responding to Identity Crime on the Internet. *International Journal of Cyber-Security and Digital Forensics*. [Online]. 1(2), pp. 67-74. Available: http://sdiwc.net/security-journal/Browse-Archive.php?ptid=1&ptsid=66&vnum=1&inum=2
58. W. Goucher, "Being a cybercrime victim," *Computer Fraud & Security*, vol. 10, pp 16-18, Oct. 2010.
59. United States General Accounting Office, "Identity Fraud: Information on prevalence, cost, and Internet impact is limited," [Online]. Available: http://www.gao.gov/archive/1998/gg98100b.pdf. [Accessed: Apr. 17, 2015].
60. A. Muurashat, "Australia's accession to the cybercrime convention: is the convention still relevant in combating cybercrime in the era of botnets and obfuscation crime tools?," *University of New South Wales Law Journal*, vol.33, no. 2, pp. 431-473, Mar. 2011.
61. S. Abraham, and I. Chengulur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Society*, vol. 32, no. 3, pp. 183-196, Aug, 2010.
62. B. Zheng, P. Bueno, P. Kashyap, and A. Wosotowsky, "The New Era of Botnets," McAfee. [Online]. Available: http://www.mcafee.com/au/resources/white-papers/wp-new-era-of-botnets.pdf. [Accessed: Feb. 13, 2015].
63. C. Wilson, "Botnets, cybercrime, and cyber terrorism: vulnerabilities and policy issues for congress," CRS Report for Congress. [Online]. Available: https://www.fas.org/sgp/crs/terror/RL32114.pdf. [Accessed: Apr. 17, 2015].
64. European Union, "Communication from the Commission to the European Parliament, The Council and the Committee of the regions – Towards a general policy on the fight against cybercrime," [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52007DC0267. [Accessed: Apr. 25, 2015].
65. S. Stankovic, and D. Simic, "Defense Strategies Against Modern Botnets," *International Journal of Computer Science and Information Security*, vol. 2, no. 1. pp. 1-7, Jun. 2009.

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(1): 10-20
The Society of Digital Information and Wireless Communications, 2016 (ISSN: 2305-0012)

A Discrete Wavelet Transform Approach for Enhanced Security in Image Steganography

Ashley S. Kelsey, Cajetan M. Akujuobi

Department of Electrical and Computer Engineering, Prairie View A&M University, USA
100 University Drive, Prairie View, TX 77446
akelsey@student.pvamu.edu, cmakujuobi@pvamu.edu

ABSTRACT

The magnitude of the growth in the Internet combined with the increase in technological innovations pose serious threats to the process of digital data transmission. The government, military, small and large businesses and corporations, and individuals transmit private or confidential information over public and private networks every day creating a need for preserving the confidentiality of this information. But because of the growth of the Internet and technology, the security of information and data being transmitted and received is at risk of being copied, destroyed, and/or modified. In this paper, an advanced, multi-level security steganographic method will be presented. The proposed system combines two hiding methods, namely Cryptography and Steganography. Cryptography involves encrypting the secret data or information into a non-recognizable cipher. Steganography is then employed using the Discrete Wavelet Transform (DWT) method, to embed the encrypted data into a cover medium to hide its existence. The proposed system employs wavelet-based fusion while manipulating the embedding strength factors in order to improve the overall hiding capacity, imperceptibility, robustness and security of the final steganographic image.

KEYWORDS

Cryptography, Discrete Wavelet Transform (DWT), embedding strength factors, hiding capacity, imperceptibility, robustness, security, steganography, wavelet fusion.

1 INTRODUCTION

STEGANOGRAPHY, also known as data hiding, is the science of secret communication on a public or private network [1]. Data hiding has become very important and useful recently because of the advancement of technology and ability to hack or falsely obtain data or information [2].

Three popular techniques for hiding data are cryptography, watermarking, and steganography. Cryptography is a data hiding technique in which data is encrypted with a key so it cannot be read or understood by a person who does not have the key. The data is not hidden to eavesdroppers and consequently, attackers can intercept the message or data and attempt to decipher the encrypted message [3]. Watermarking is an ownership technique in which a watermark is embedded for copyright protection purposes, temper proofing, and authentication purposes. However, of all three techniques, the steganography technique has proven to be the most trusted and also has the ability to use the other techniques in order to provide added security. The main goal of steganography is to hide data in a medium (images, videos, etc.), where the data or information embedded in the medium is undetectable. A layered approach is imperative because there is not a system that exists, in which complete security from all attacks is guaranteed [4]. Therefore, a system combining watermarking, cryptography, steganography, or other techniques creating layers of security is desired.

There are four characteristics of data hiding, namely imperceptibility, hiding capacity, security, and robustness. Imperceptibility means that the human eyes cannot distinguish if there is data or

information hidden in the image. Hiding capacity refers to the amount of data that can be embedded in the image without significantly decreasing the quality of the image. Security refers to the inability of an eavesdropper to detect the hidden information embedded in the image or extract the secret data from the cover image. Robustness means the data or information should be able to be recovered with a small amount of errors. This paper focuses on presenting a steganography technique that improves all four of these characteristics. This paper is organized as follows: Section 2 will give details about the objectives of this work, Section 3 introduces the proposed algorithm, Section 4 will evaluate and discuss the results of the simulations, Section 5 will discuss the conclusions, and Section 6 will discuss future work.

2 OBJECTIVES

In this paper, there are specific objectives set forth in order to create a highly efficient and secure steganographic method to improve upon current steganographic techniques. These objectives are as follows:

A. Develop an algorithm to embed data into a cover image in the wavelet domain.
B. Develop an algorithm that incorporates encryption to add an additional layer of security but does not negatively affect the quality of the final stego-image.
C. Develop an algorithm that will improve the overall imperceptibility, hiding capacity, security, and robustness of the current steganographic method.
D. Manipulate the embedding strength factors of the coefficients in the wavelet fusion process in order to determine which numerical values will hide the data the most efficient as well as give the best MSE, PSNR, and entropy values.

3 RESEARCH METHOD

There have been numerous research efforts dedicated to the analysis of past and current steganographic methods because of the importance of securing important data or information [1], [2], [5], [6], [7]. The most popular transform hiding steganography techniques are based on the discrete Fourier transform (DFT), the discrete cosine transform (DCT), the discrete wavelet transform (DWT), the singular value decomposition (SVD), the discrete Hadamard transform (DHT) [1] and the Integer Lifting Wavelet Transform (IntLWT) [5]. Previous research prove that discrete wavelet transform produces the best results of these techniques in terms of imperceptibility, security, hiding capacity, and robustness [6], [7], [8], [9]. Kumar et al. [3], Tong et al. [7], Ulrich [8], Shakkakarmi [9], Kumar et al. [10], and Lai et al. [10] propose methods based on the discrete wavelet transform. The results of these methods outperform results of the previously stated methods and prove the use of wavelets has a higher hiding capacity as well. Muttoo et al. [1], Ulrich [8], Shakhakarmi et al. [9], Lai et al. [11], and Patil et al. [12] propose methods in which they perform comparative wavelet studies. The results of these comparative studies show the Haar wavelet outperforms other wavelets when applied to the steganography process. These methods prove that DWT is more efficient for the steganographic process and in addition, Haar wavelet proved to be the most efficient wavelet for the steganography process.

The goal of this paper is to introduce a multi-level security-based steganography system in which cryptography and steganography are combined to provide an overall more efficient and secure data hiding method. The proposed system involves combining encryption, the Discrete Wavelet Transform, and wavelet fusion to hide a payload (secret image) inside a cover image in order to completely hide the existence of the encrypted payload (secret image).

3.1 The Discrete Wavelet Transform

Wavelets are defined as functions over a finite interval. The wavelet transform represents an arbitrary function as a superposition of a set of wavelets or basis functions, which are obtained from the mother wavelet by dilations and translations. The wavelet transform converts an image from time or spatial domain to the frequency domain. The wavelet transform can be determined by repeated filtering of the coefficients of the image row-by-row and column-by-column, which separates the high frequency and low frequency information of the image. The input image is convolved with a series of high and low pass filters applied first to the rows and then to the columns resulting in four bands. The four bands obtained are the approximate band (LL), vertical detail band (LH), horizontal detail band (HL), and diagonal detail band (HH). The approximation band contains the low frequency wavelet coefficients, which contains the significant part of the spatial domain image. The other three detail bands contain the edge details of the spatial domain image. The image can be decomposed further by applying another level of decomposition to the existing LL subband [13]. The DWT process allows independent processing of the coefficients without significant perceptible modifications to the original image, hence the reason DWT is a better technique for the steganography process. The process of one-level discrete wavelet transform applied to a two-dimensional image is shown in Figure 1.

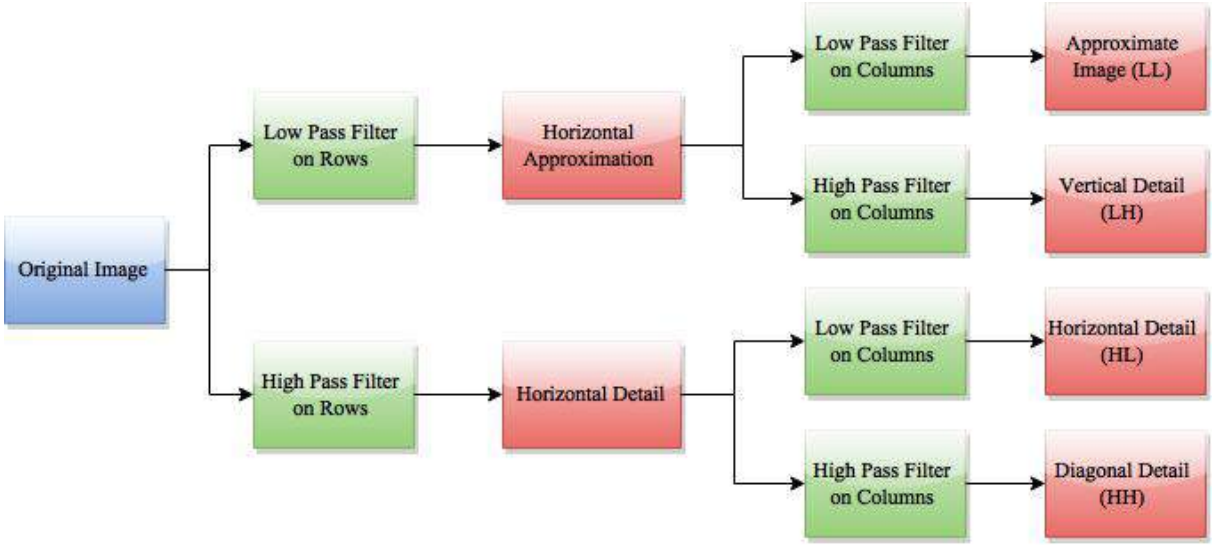


Figure. 1. One-level discrete wavelet transform applied to a two-dimensional image.

3.2 Wavelet Fusion

The proposed algorithm is based on the technique proposed by Reddy et al. [2], Patil et al. [12], and Tolba et al. [14]. The technique behind the proposed algorithm is wavelet-based fusion. Wavelet-based fusion merges the wavelet decomposition of the normalized cover image and the wavelet decomposition of the secret image and fuses the two resulting images into one single image. Usually, the integer range of pixels is (0, 255) but normalization transforms the pixel range of the image to floating point values between 0.0 and 1.0. The process of normalization is completed in order to prevent problems pertaining to overflow and underflow, ensuring the reconstructed pixels does not go out of range preventing the addition of unnecessary noise. The new normalized pixel values are input into the floating-point filters and results in the reconstruction

of the transformed image. This reconstructed image has a better accuracy. Both the cover image and the secret image are then converted into the DWT domain to increase the level of security. The resultant matrix can be obtained by Equation (1).

$$F(x,y) = \alpha C(x,y) + \beta P(x,y) \quad (1)$$

where $\alpha + \beta \cong 1$, F is the modified DWT coefficients, C is the DWT coefficients of the cover image, and P is the DWT coefficients of the payload (secret image). Alpha and Beta are the embedding strength factors chosen to ensure the payload or secret image is not predominantly seen in the final stego-image. Once the fusion process is completed, inverse discrete wavelet transform (IDWT) is applied. After renormalization is completed the final result is the stego-image in the spatial domain.

3.3 Proposed Algorithm

The proposed system consists of two phases: the embedding phase and the extraction phase. For the embedding phase, first the payload (secret image) and cover images are selected. Both images are normalized and 3-level Haar discrete wavelet transform is performed. Previous methods use 2-level DWT [2,10], but the proposed method increases from 2-level to 3-level DWT in order to increase the hiding capacity and to improve upon the imperceptibility as well. The payload is encrypted and then the coefficients of both the encrypted payload (secret image) and the cover image are obtained. The values of alpha and beta (the embedding strength factors) are manipulated in order to determine the values that will completely hide the payload in the selected cover image and finally the coefficients are fused together. In the work of Reddy et al. [2], they used $\alpha + \beta = 1$; where α is the embedding strength factor of the cover image and β is the embedding strength factor of the payload. In the proposed algorithm, we found that when α is constant at 1 and β is kept as small as possible, the performance improved. Please see Section 4 for more discussions on this topic. Three-level IDWT is performed to reconstruct the image. The image is then denormalized and the final stego-image is obtained. The extraction process is the reverse of the embedding process.

3.4 Embedding and Extracting Algorithm

The embedding algorithm and the data extraction algorithm for the proposed method is as follows:

Embedding algorithm:
Input: Payload image, P, and cover image, C.
Output: Stego-image, S.

- Choose the payload image, P, and the cover image, C
- Normalize payload image, P, and cover image, C, so the pixels vary between 0.0 and 1.0
- Encrypt payload image, P
- Transform C and P into 3 levels of decomposition using the Haar wavelet
- Wavelet fusion of DWT coefficients of P and C
- Perform the 3-level IDWT of all the subbands of the fused image
- Denormalize the fused image
- The final stego-image, S, is generated

A block diagram illustrating the embedding process is shown in Figure 2 and the extraction process is illustrated in Figure 3.

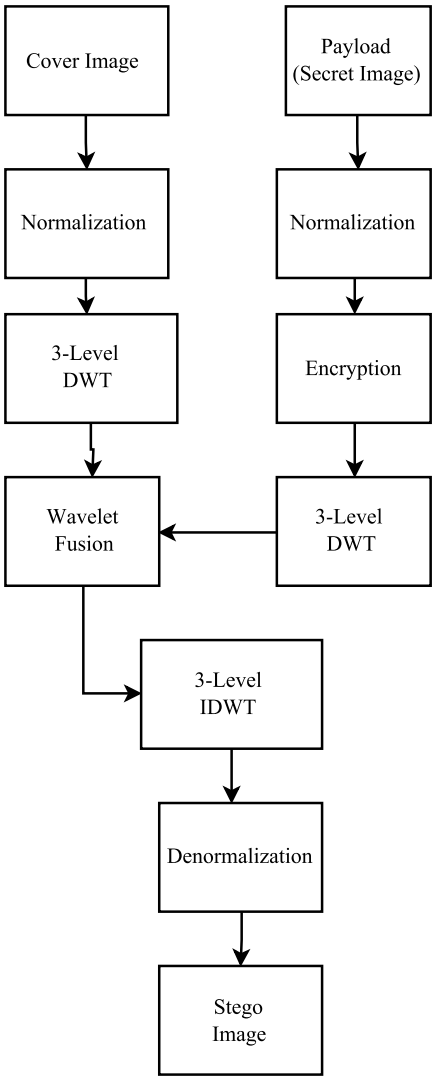


Figure. 2. Embedding process.

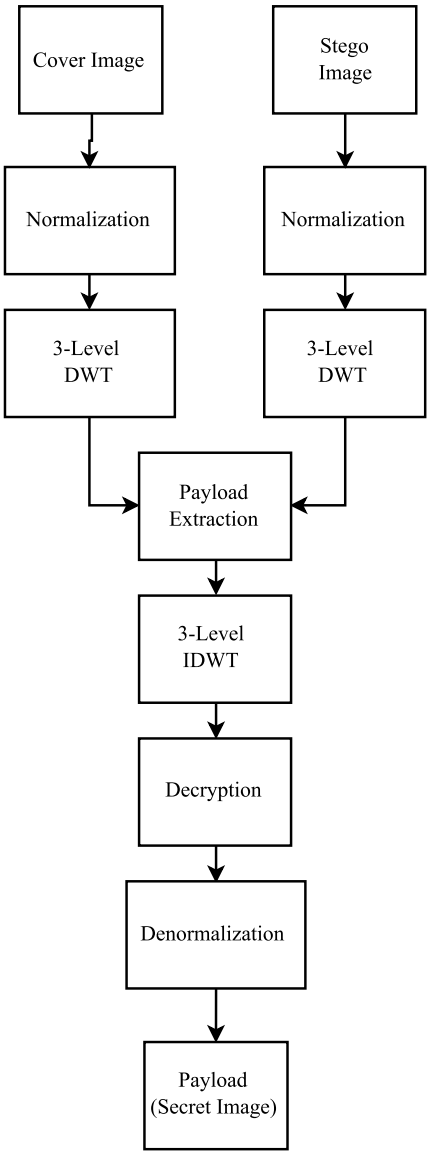


Figure. 3. Data extraction process.

Data extraction algorithm:
Input: Stego-image, S.
Output: Payload message/image, P.

- Normalize the stego-image, S, and cover image, C
- Transform S and C into 3 levels of wavelet decomposition
- Subtract the DWT coefficients of C from the DWT coefficients of S to get the DWT coefficients of P
- Apply 3-level IDWT to the subbands of P
- Decrypt P
- Denormalize the payload, P

Payload image, P, is obtained

A total of five images were downloaded from The University of Southern California's School of Engineering's online image database [15]. In addition to these images, an image with an actual message is created in order to determine if the message can be deciphered after performing encryption, three-level DWT, and wavelet fusion. All of the images used in the study were converted to 512 x 512. MATLAB R2015a version 7.0 was used in order to create a code based on the proposed algorithm. Table 1 shows the image combinations and their corresponding values. The selected payloads (secret images) and the corresponding cover images are shown in Figure 4.

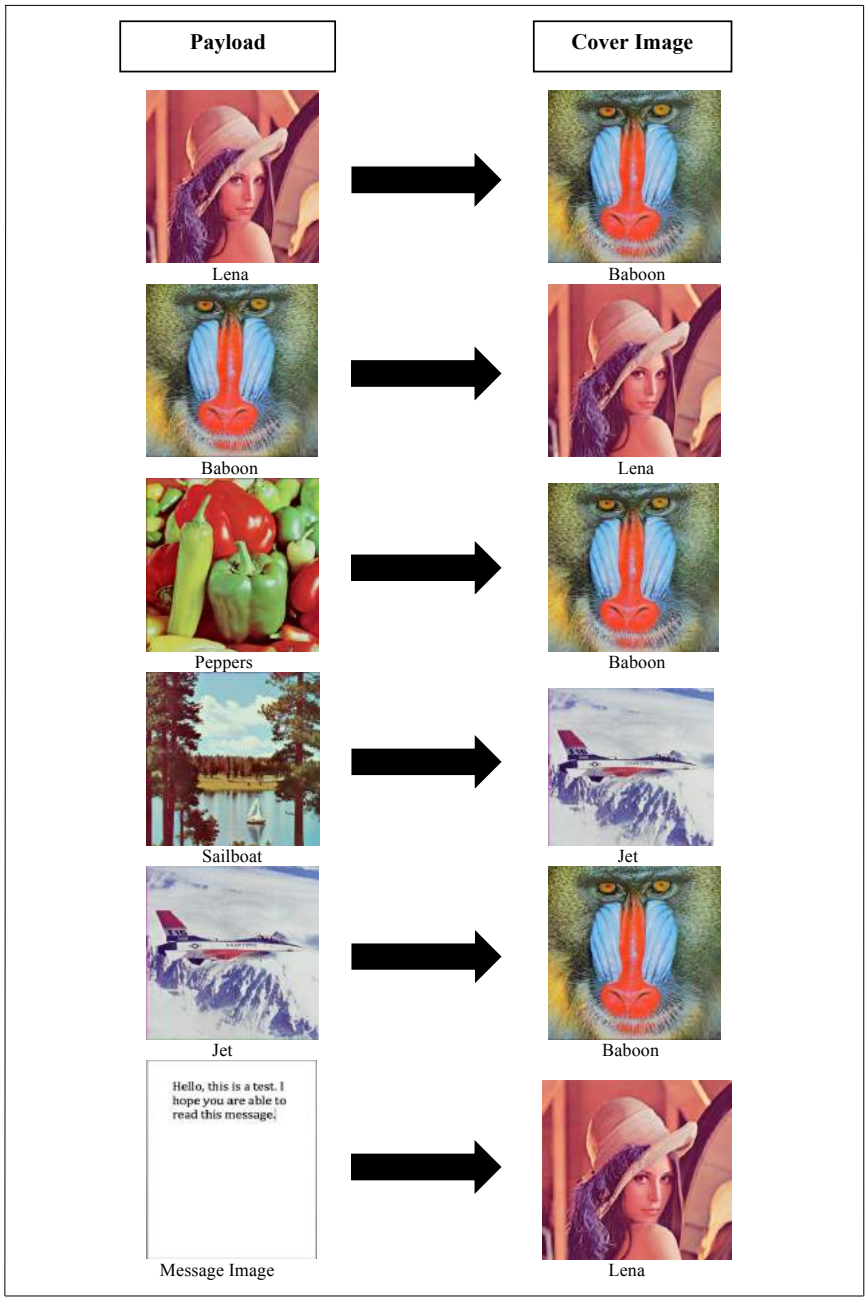


Figure. 4. Selected secret images and corresponding cover images.

Table 1. Combinations of images and their corresponding values.

Combination #	Payload (Secret Image)	Cover Image
1	Lena	Baboon
2	Baboon	Lena
3	Peppers	Baboon
4	Sailboat	Jet
5	Jet	Baboon
6	Message Image	Lena

4 RESULTS AND DISCUSSIONS

4.1 Performance Metrics

Steganography is defined as stated in Section 1. However, steganography is said to be secure if the existence of the information/data hidden in the cover image is undetectable, meaning an individual cannot

distinguish the difference between the original cover image and final embedded stego image. To determine the security of the proposed steganographic method, there are three widely used metrics used: MSE, PSNR, and Entropy.

The mean squared error (MSE) is used to calculate the difference between the original cover image and the final stego-image. The equation for the MSE is shown below:

$$MSE = \sum\sum \frac{(Cover(i,j) - stego(i,j))^2}{M\ x\ N} \qquad (2)$$

where $Cover(i,j)$ represents the image pixel value at position (i,j) for the cover image and $stego(i,j)$ represents the pixel value at position (i,j) after the payload has been embedded. The MSE is used to calculate the Peaked Signal to Noise Ratio (PSNR). The PSNR is calculated in order to determine the quality of the stego-image with respect to the original cover image. The higher the PSNR the better the quality of the final stego-image. A higher PSNR is achieved by minimizing the differences between the original cover image and final stego image; as a result, the MSE is minimized and the PSNR increases. Hence, the secret image is more efficiently hidden in the cover image. The PSNR is given by the following equation:

$$PSNR = 10log_{10}\frac{255}{\sqrt{MSE}} \qquad (3)$$

The Kullback-Liebler Divergence (KLDiv) also known as the relative entropy is a statistical measure of the distance between two probability distributions [10]. The entropy is calculated in order to quantify the irregularity between the original image and the final stego-image. The desired entropy is zero or as close to zero as possible, meaning there is no significant difference between the cover image and the final stego-image. The relative entropy is defined as:

$$D(px||qy) = \sum_{g\ \varepsilon\ G}[px(g)\log(\frac{px(g)}{qy(g)}] \qquad (4)$$

where X and Y are random variables representing the cover image and stego image, p_x and q_y represent the probability mass functions of x and y, and $g\varepsilon G \approx \{0,1,2,\ldots,255\}$ is the pixel value. The security of the steganography process is considered perfect if $D(px||qy) = 0$.

4.2 Embedding Strength Factor Manipulation and Results

Reddy et al. [2] proposed $\alpha + \beta = 1$, but through simulations it was determined the cover image more efficiently covered the payload and the results of the performance metrics were increased (further discussed in Section 5) when alpha was kept constant at 1 and beta was kept small. Five sets of beta were chosen for the simulations: 0.1, 0.01, 0.05, 0.001, and 0.005. From the simulations, it was observed that in order to completely and efficiently cover the payload the embedding strength factor of the cover image (alpha) should be as strong as possible and the embedding strength factor of the payload (beta) needs to be as small as possible. The MSE, PSNR, and entropy results of the simulations comparing the manipulations of beta are illustrated in Figures 5, 6, and 7. Table 2 compares the MSE, PSNR, and entropy results for the six payload and cover image combinations.

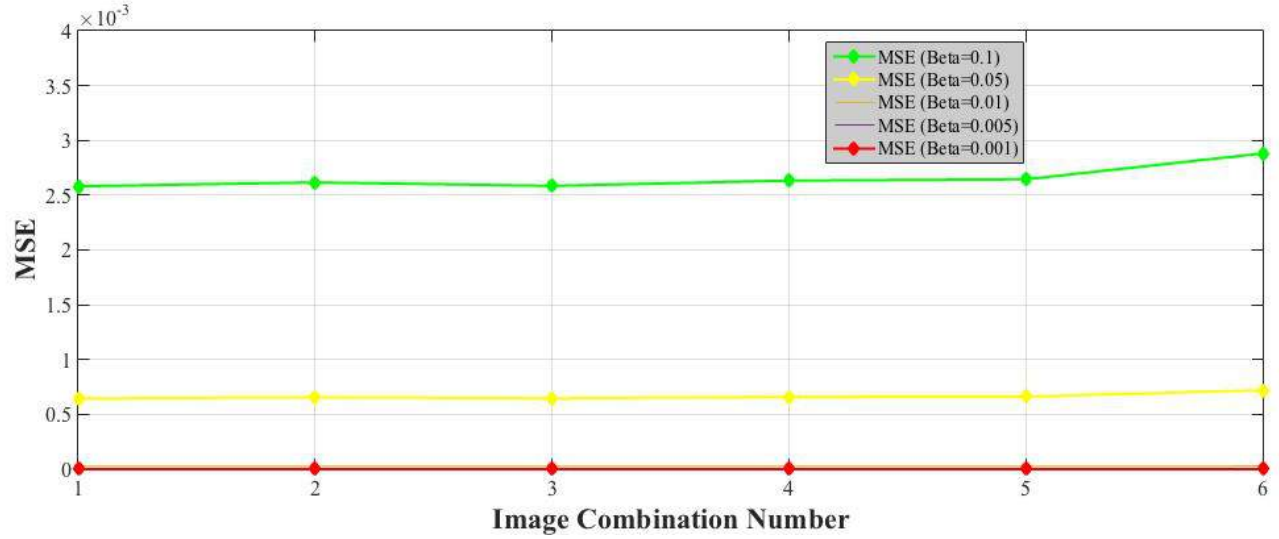


Figure. 5. MSE data from the simulations.

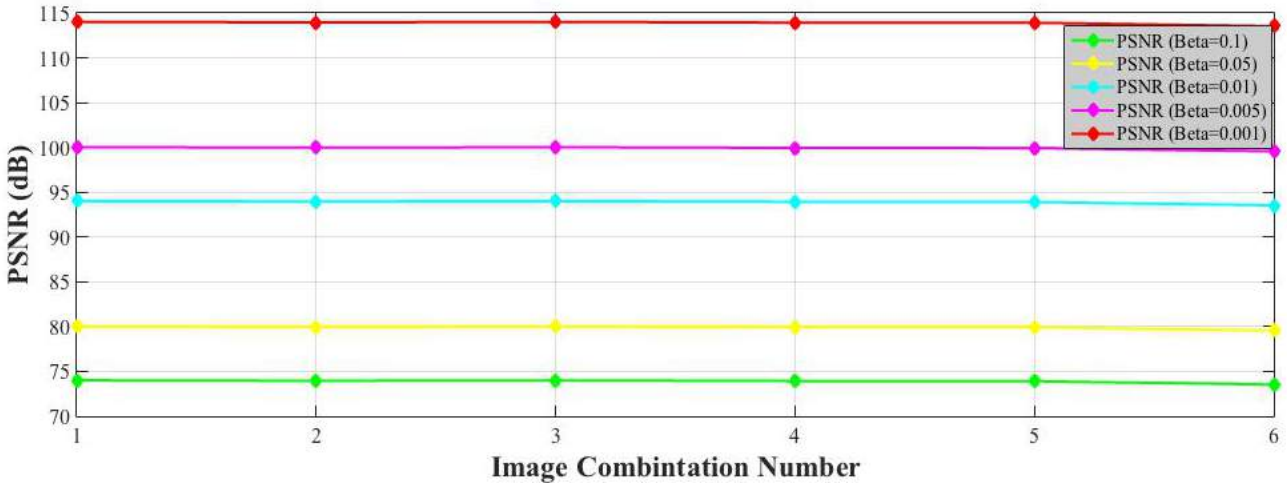


Figure. 6. PSNR data from the simulations.

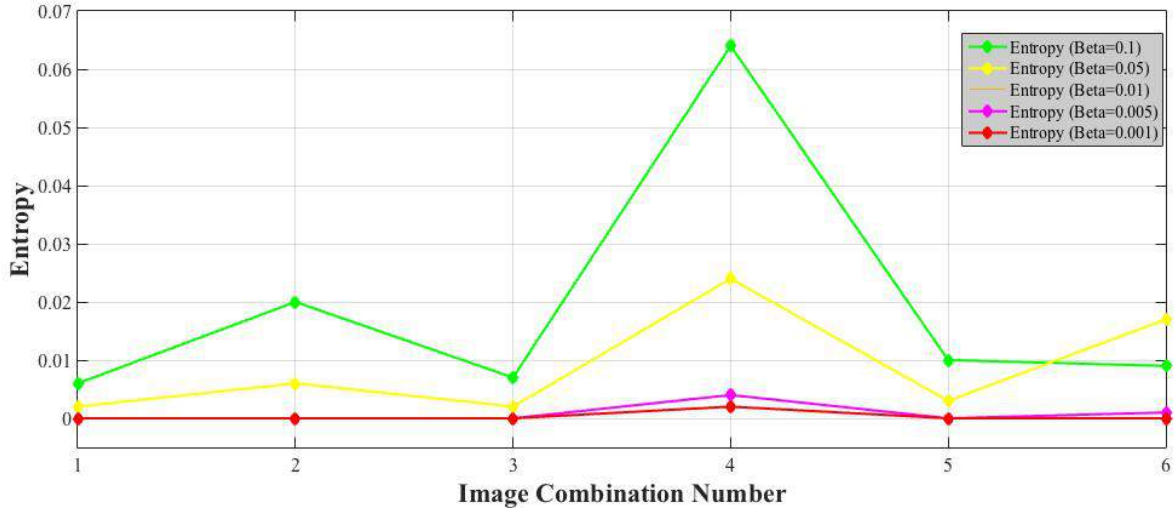


Figure. 7. Entropy data from the simulations.

4.3 Discussions

From the results of the parameters in Table 1 and consequently the plots in Figures 5, 6, and 7, the following observations were noted:
The analysis with wavelets produced better results than methods not using the DWT. The embedding strength factor of 0.001 obtained better results in all areas, MSE, PSNR, and entropy. Hence, better results are obtained when $\alpha + \beta \cong 1$. The quality of final stego-image with respect to the original cover image was good, and as a result imperceptibility is increased.

Table 2. PSNR, MSE, and entropy data from the simulations.

Cover Image	Secret Image	MSE	PSNR	Entropy	Beta
Baboon	Lena	0.000645156	80.034 15471	0.002	0.05
Lena	Baboon	0.000654182	79.973 81803	0.006	0.05
Baboon	Peppers	0.000646186	80.027 22783	0.002	0.05
Jet	Sailboat	0.000658254	79.946 86891	0.024	0.05
Baboon	Jet	0.000661304	79.926 79267	0.003	0.05
Lena	Message Image	0.000720196	79.556 2963	0.017	0.05
Baboon	Lena	2.5806 2E-05	94.013 5548	0	0.01
Lena	Baboon	2.6167 3E-05	93.953 21812	0	0.01
Baboon	Peppers	2.5847 4E-05	94.006 62792	0	0.01
Jet	Sailboat	2.6330 2E-05	93.926 269	0.002	0.01
Baboon	Jet	2.6452 2E-05	93.906 19275	0	0.01
Lena	Message Image	0.0000 288	93.535 696	0.001	0.01
Baboon	Lena	6.4515 6E-06	100.03 41547	0	0.005
Lena	Baboon	6.5418 2E-06	99.973 81803	0	0.005
Baboon	Peppers	6.4618 6E-06	100.02 72278	0	0.005
Jet	Sailboat	6.5825 4E-06	99.946 86891	0.004	0.005
Baboon	Jet	6.6130 4E-06	99.926 79267	0	0.005
Lena	Message Image	7.2019 6E-06	99.556 2963	0.001	0.005
Baboon	Lena	2.5806 2E-07	114.01 35548	0	0.001
Lena	Baboon	2.6167 3E-07	113.95 32181	0	0.001
Baboon	Peppers	2.5847 4E-07	114.00 66279	0	0.001
Jet	Sailboat	2.6330 2E-07	113.92 6269	0.002	0.001
Baboon	Jet	2.6452 2E-07	113.90 61928	0	0.001
Lena	Message Image	2.8807 8E-07	113.53 56964	0	0.001
Baboon	Lena	0.0025 80625	74.013 5548	0.006	0.1
Lena	Baboon	0.0026 16728	73.953 21812	0.02	0.1
Baboon	Peppers	0.0025 84744	74.006 62792	0.007	0.1
Jet	Sailboat	0.0026 33016	73.926 269	0.064	0.1
Baboon	Jet	0.0026 45216	73.906 19275	0.01	0.1
Lena	Message Image	0.0028 80784	73.535 69638	0.009	0.1

An efficient encryption method was proposed and tested to ensure encryption would not have a significant negative effect on the quality of the final stego-image and resulted in an added layer of security. The discrete wavelet transform allows for more data to be able to be hidden in the cover image without negatively affecting the overall quality of the image and as a result increases the hiding capacity of the proposed method. The discrete wavelet transform makes the embedding and extracting process easier which increases the overall robustness of the proposed method as well because the extracted payload still has good quality after encryption, DWT, and wavelet fusion are performed. Furthermore, the message is still able to be deciphered after the extraction phase in which the payload is extracted from the final stego image.

The proposed algorithm produces better results because of the following reasons:

1. The use of wavelets helped decrease the amount of noise added to the image normally caused by other steganographic methods.
2. The increase from 2-level 2-dimensional DWT decomposition to 3-level 2-dimensional DWT

decomposition helped reduce the amount of noise added from the embedding of one image into another.

3. Adding encryption to the proposed algorithm added another layer of security to the process. If a third party obtains the stego image, DWT and cryptanalysis will have to be performed provided the third party is able to determine the presence of the hidden data in the image.
4. Minimizing the embedding strength factor beta, increases the imperceptibility of the final stego-image, which ultimately increases the overall security of the image.

5 CONCLUSIONS

The proposed method had minimal to no effect on the quality of the images, making it hard for eavesdroppers to determine the presence of data hidden in the image. The added encryption security layer also makes it difficult for eavesdroppers to extract the information provided they are even able to determine there is data hidden in the image. The proposed method improves the overall imperceptibility, security, hiding capacity, and robustness and creates a more secure and efficient steganographic method. From these observations, the objectives of this work were met.

6 FUTURE WORK

Future research will focus on creating a user-friendly program in which the user is able to choose the information they would like to hide, choose an encryption key, and in response the program chooses the most efficient image to use for the chosen secret data/information. The program will perform encryption, DWT, and wavelet fusion (embedding). The recipient will only need to enter the shared encryption key and the secret data will be automatically extracted from the image.

Future work will also focus on determining the correlation between alpha and beta and the MSE and PSNR. Knowing these values before running the simulations could help predict the efficiency of the proposed method and the resulting image quality.

Improving steganographic methods will not only increase the security of transmitting secret data/information across a public or private network, but will also increase the intelligence of steganography for purposes of protecting our country. Understanding steganography methods can help intelligence agencies or military personnel intercept messages from foreign countries and extract the secret data/information in order to be constantly be informed about planned attacks or negative breaches to our country's assets, information, and/or security. Furthermore, understanding steganographic techniques can also help protect business/corporations, individuals, and the government protect proprietary or sensitive information.

REFERENCES

1. Muttoo S.K., Kumar S.: Robust Source Coding Steganographic Technique Using Wavelet Transforms. BVICAM. 1(2), pp. 91-96. (2009). Available: http://bvicam.ac.in/bijit/downloads/pdf/issue2/02.pdf
2. Reddy H.S.M., Raja K.B.: High Capacity and Security Steganography Using Discrete Wavelet Transform. IJCSS. 3(6), pp. 462-472. (2009). Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.8140&rep=rep1&type=pdf
3. Stallings W.: Cryptography and Network Security: Principles and Practice. 5th ed., Upper Saddle River, N.Y.: Prentice Hall, (2011).
4. Akujuobi C.M., Ampah N.K., Sadiku M.N.O.: An Intrusion Detection Technique Based on Change in Hurst Parameter with Application to Network Security. IJCSNS. 7(5), pp. 55-64. (2007).
5. Seyyedi S.A., Ivanov N.: An Adaptive Steganographic Method in Frequency Domain Based on Statistical Metrics of Image. IJCSDF. 3(1), pp. 63-71. (2014).
6. Kumar S., Muttoo S.K.: A Comparative Study of Image Steganography in Wavelet Domain. IJCSMC. 2(2), pp. 91-101. Available: http://ijcsmc.com/docs/papers/February2013/V2I2201316.pdf. (2013).
7. Tong L., Zheng-ding Q.: A DWT-based Color Images Steganography Scheme. IEEE ICSP. 2, pp. 1568-1571. Available:

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1180096. (2002).

8. Ulrich G.: "Robust Source Coding with Generalized T-codes," PhD. thesis, C.S., The Univ. of Auckland, New Zealand. (1998).
9. Shakkakarmi N.: Quantitative Multiscale Analysis using Different Wavelets in 1D Voice Signal and 2D Image. IJCSI. 9(2), pp. Available: http://arxiv.org/pdf/1203.4035.pdf. (2012).
10. Kumar S., Muttoo S.K.: Image Steganography Based on Wavelet Families. IJCEIT. 02(02), pp. 1-9. Available: http://scitechnol.com/image-steganography-based-on-wavelet-families-oyKL.php?article_id=719#>. (2013).
11. Lai B., Chang L.: Adaptive Data Hiding for Binary Images Based on Haar Discrete Wavelet Transform. PSIVT. LNCS. 4319, pp. 1085-1093. Available: http://link.springer.com/chapter/10.1007%2F11949534_109. (2006).
12. Patil S., Chandel G.S.: Performance Analysis of Steganography Based on 5-Wavelet Families by 4 Levels - DWT. IJARCSMS. 1(7), pp. 175-83. Available: http://www.ijarcsms.com/docs/paper/volume1/issue7/V1I7-0028.pdf. (2013).
13. Sheng Y.: Wavelet Transform in The Transforms and Applications Handbook. 2nd ed. Alexander D. Poularikas, Ed. Boca Raton, Fl.: CRC Press LLC (2000).
14. Tolba M.F., Ghonemy M.A.-S., Taha I.A.-H., Khalifa A.S.: High Capacity Image Steganography Using Wavelet-Based Fusion. Computers and Communications, Proceedings. ISCC. Ninth IEEE Symposium on Computers and Communications. 1, pp. 430-435. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1358443. (2004).
15. The USC-SIPI Image Database. Available: http://sipi.usc.edu/database/database.php?volume=misc&image=15#top.

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(1): 21-29
The Society of Digital Information and Wireless Communications, 2016 (ISSN: 2305-0012)

Cyber Operation Planning and Operational Design

Muhammer Karaman, Hayrettin Catalkaya, Ahmet Zeki Gerehan and Kerim Goztepe
Operations and Intelligence Turkish Army War College
War Colleges Command, 4. Levent/Istanbul, 34330, Turkey
mkaraman@harpak.edu.tr; hcatalkaya@harpak.edu.tr; azgerehan@harpak.edu.tr;
d065006003@sakarya.edu.tr

ABSTRACT

Improving ICT infrastructure, dramatic increase in internet usage and increasing dependence on networks have carried with cyber risks and threats. Complex, shape shifting and emerging risks and threats have systematically paved the way for cyberspace to emerge as a new domain after land, air, maritime and space. It is obvious enough that cyber threats probably continue to take part in global cyber theatre for years. However, it is sometimes hard to pinpoint at first a specific axis of cyber threats; they are generally varied merely from a simple computer code to systematic cyber strikes like targeted cyber attacks, cyber terrorism and industrial espionage activities. Due to the exponential use of cyberspace and the complex nature of cyber attacks, along with the multivariable cost they cause, it becomes a requirement for operation planners to handle cyber operations and the problems in this sphere in an operational design process. In this study, we tried to handle cyber operations in operational design process in order to comprehend, visualize and enlighten complex cyber incidents holistically and present preventive and systematic approaches by proposing a cyber operational design model. By presenting such model, we aim to help operation planners understand the complexity of cyber operations, show the advantage of using factor and center of gravity analysis (COG) that is generally handled in military decision making process (MDMP) and finally help the technical personnel to have an understanding of operational planning. With the cyber operational design presented as a sample in this study, we plan to provide the commanders with a comprehensive approach in cyber operations.

KEYWORDS

Cyberspace operations, operational design, cyber threats, cyber operational design, military decision making process (MDMP).

1 INTRODUCTION

Throughout history, there has always been a struggle of force among communities. Struggles, conflicts or fights have managed to reach up to modern times with different forms of tools, tactics and techniques [1]. Strategies are developed to direct and command armies and also envision the enemy and its tactics. These strategies mainly vary depending on the commanders' intents that form the desired end state on the enemy. When we compare two outstanding military strategists, Sun Tzu and Clausewitz, and their work in order, "The Art of War" and "On War", we can see some differences in them. For example, the concepts of Sun Tzu generally imply that the force should be the last resort to apply. If the enemy is defeated without fighting that is better or to take a state untouched is recommended by him [2] On the other hand, Clausewitz emphasizes theoretically the importance of "total war" or "absolute war". As it is understood, he defines a war that is waged against the enemy with all resources and momentum until the enemy is wiped out [2]. In today's complex and multi-dimensional security environment, commanders need to analyze the strategies and also take the new variables like cyberspace, which is emerging as a new domain after air, land, maritime and space [3], into account. The operational environment, comprising of friend, enemy and neutral systems, has been experiencing a new factor, cyberspace, that supports and interacts with operational variables like political, military, economic, social, information, infrastructure etc [4] [5]. The operational environment (OE) is not separate from information system infrastructure due to the large amount of information running on networks [3]. Evolving technology and the increasing use of social networks has necessitated the governments

and institutions to have at first the situational awareness and then more than that.

Particularly, increasing use of information communication technologies (ICT), smart devices (phones and tablets) and over three billion people having internet access have popularized the use of blogs and social networks[6][7]. And along with these facts, cyberspace has become a suitable area for criminals and terrorist organizations [8]. For example, ISIS has been using the social media to spread its ideology and message after it seized Mosul, Iraq's second-largest city, [9]. In particular, ISIS was able to succeed in creating an atmosphere of fear in Iraq by releasing the execution videos and photos on social networks like Twitter and YouTube [10]. The power of social networks, during elections, street incidents in repressive regimes or during natural disasters, has proved its ability to change traditional one-way media, from news agency to people. With this change in media, big news agencies also have taken advantages of user generated footage [11] As a consequence of those facts, some government actions are seen on interferences and restrictions on access to information sources especially from social networks that provide instant feeds.

In this new operational environment where it is easy to conceal itself for a long period of time, cyber wars have been waged similarly with physical ones [12]. Being as real as physical ones, cyber wars start in cyberspace and have effects and influences in real life [13]. Increasing number and diversities of cyber attacks require people, institutions and countries to take strong measures against them. These precautions range from personal actions like being aware of cyber risks, having situational awareness to strategic actions like having a national cybersecurity document, forming a computer incident response team (CIRT). More comprehensive approaches are also put into action by founding governmental and military cyber organizations to protect the assets, defense and cooperate. In these organizations, according to its level, vulnerability assessment, cyber incident handling, configuration management and cyber training activities are handled. As an institution, military organizations must ensure that its cyber assets are being protected and must be prepared by adapting its procedures, plans and doctrines to operate in this evolving and ambiguous area, cyberspace, where it is replete with criminal organizations and individuals [3]. The targets of cyber attacks can vary according to the causes and desired end states which the planners or perpetrators struggle to attain. Qiao and Wang, The Two Chinese Strategies, define the battlefield: "The battlefield is next to you and the enemy is on the network. Only there is no smell of gunpowder or the odor of blood" [14].

In this study, we tried to adapt cyber operations to fit in an operational design and named it cyber operational design in order to help cyber and operation planners to understand each other better and share this new OE in common. Operational design is generally done before planning to visualize the enemy and operation environment and deal with the ill structured problems in a more comprehensive way [15]. In section two we emphasized the need of cyber operational design with mentioning about the well known cyber attacks having strategic objectives. In this section we also defined our study that it is not based on a real cyberspace operation. We haven't discussed about the legality of cyberspace operations in this section. In section 3, we mentioned about operation planning, military decision making process (MDMP), operational art, operational design and its elements. We also prepared a sample cyber factor analysis that sheds light on cyber operational design explained in the following section. In section 4, we defined the relations between cyberspace operations and cyber operational design and the need of understanding of these two. In this section we prepared a cognitive map of cyber operational design by the help of factor analysis and cyber center of gravity. In conclusion, we have drawn attention to the need of cyber operational design and by this we have shown the importance of bringing cyber specialists and operation planners together for better planning of military operations.

2 METHODOLOGY

Understanding a complex operational environment such as cyber warfare requires a combination of art and science and ability to blend knowledge,

experience, intuition, and critical thinking that are essential to operational design with analytical methods and tools that support detailed planning. [15]. In this study we assume that cyber operations (defence, active defense or offense) have become an integral planning factor in operational and strategic operations of countries or a supplementary tool in reaching strategic objectives. We reach this data from some cyber and intelligence related incidents that quite many professionals call them "cyber warfare" One of the leading cyber incidents is Stuxnet that intended to disrupt a country's nuclear facilities and it is widely believed that it is driven by a nation or nations having a strategic objectives. Other cyber warfare and intelligence activities can be Flame, Duqu, Red October, Regin and so on. Some of these are believed to be initiated by intelligence organizations and some are also nation sponsored. Due to the complexity of cyberspace and lack of enough legal evidence on attribution to a specific source, they are not yet rightly ascribed to a source or structure.

In our study, we will not discuss the legality of waging cyber warfare to an organization, country or enemy and we will not probe the philosophy of just or unjust war. We are interested in the process of planning cyberspace operations (CO) alone or as a part of another operation. We also emphasize that a clear definition of jobs related to cyber operations in military organizations should be prepared in detail and legal issues both in government and institutional level must entitle the commanders and operation planners to act freely within the boundaries of a legal framework.

In this paper, we haven't planned a real cyber operation and analyzed a previously planned cyber operation either. We struggle to adapt cyber operations to take advantage of operational design, operational planning and military decision making process (MDMP) and used the elements of operational design to fit cyberspace operations (CO) like cyber line of operations (CLOO), cyber center of gravity (CCOG), cyber decisive points (CDC) and cyber desired end state. While there are also some other elements of operational design, we haven't analyzed all of them here. Our study can be better executed in operational and strategic level unaided or in tactical level as a part of a higher command. In our study, we have assumed that the complex security environment that we are currently living in, the interoperability, joint operations and cutting-edge technology are going to play a significant role. What we have deducted from our assumption are to understand operation planners and cyber professionals each other better in order to have a thorough, well prepared cyber operation planning and to draw also a cyber situational awareness to both technical and staff personnel.

3 OPERATION PLANNING, MILITARY DECISION-MAKING PROCESS (MDMP)

3.1 Operation Planning

Planning is an activity that helps bring the commander's visualization into practice and forms course of actions to reach a military target [16]. Due to the ambiguous nature of military operations, many variables of the operational environment and unforeseen events necessitate the planning to be a continuous activity. According to the Field Manual 5-0, The Operations Process, planning is associated with art and firstly comprehending then visualizing a fact and putting forward the ways to reach the target. [17]. Regardless of its level, planning is an indispensable part of an every organization. To manage the available time effectively and spare maximum time to subordinates [18], parallel planning is applied during a military decision making process which is an analytical process or a checklist to carry out every element in sequence to reach a detailed document without escaping even a small point one's notice.

Operational design and operational planning are two close, concurrent elements that can be prepared by a different or same team. It may not be easy to have two different (designers and planners) teams doing these two jobs. Besides, having two separate teams may result with lack of coordination, synchronization and may harm the nature of coupling of these two. Operation planning, is a set of procedures that are needed to be started after getting a higher command's order, commander's initial guidance or directly from the situation. Operational planning can be classified in

two sections, conceptual and detailed planning [19]. In this context; while the operational design forms the conceptual planning (with a cognitive map) the military decision-making process forms the detailed planning. [19]. And FM 5-0 also describes that a powerful and useful planning is composed these two (conceptual and detailed) kinds of planning [20].

3.2 Military Decision Making Process (MDMP)

The military decision-making process (MDMP) is a continuous and recurrent process helping commander and staff to comprehend the situation, to analyze the mission, to get the commander's initial guidance, to develop course of actions [22] [23]. With the inputs of each staff officers relating with their professions, functional areas (Command and control, engineering, air defense etc.), started mission and other iterative planning methodology that integrates the activities of the commander, subordinate headquarters, staff and other partners to understand the situation. Besides, it develop and compare courses of action and select appropriate decision.

3.2.1 Factor Analysis

Factor analysis or the three-column format is sort of a checklist for staff officers to take all factors into account and deduct to do's from it. It is a frequently used methodology in MDMP and it can be used in all levels of operations. It functions as a checklist for staff officers offering planners to evaluate the operational environment, according to their functionality areas and also put forward the requirements to achieve the desired end state.
It offers a way of ordering the commander's and staffs' thought processes, and generates discipline in identifying the outputs of factor analysis. It is generally prepared in three column format (Critical Vulnerability, Deduction and Output) and named also the same. Factor analysis in table 1 is prepared in cyber means helping the CO planners to help put forward mission, critical activities about its functional area and critical vulnerabilities. The clear definition of these will also help CO and operation planners to analyze the center of gravity both of enemy and friend.

Table 1: A Sample of Cyber Factor Analysis (Three Column Format)

Mission / Critical Activity / Functional Area/ Critical Vulnerability	**Deduction**	**Output**
Lack of Talented Cyber Specialists in Military Organizations.	Being unable to envision the cyber risks.	To plan professional cyber security trainings on theory and hands on.
	Being exposed to cyber incidents and unaware of them for a long time.	To plan cybersecurity lessons in military high schools and academies.
		Station some personnel on job training to scientific organizations and institutes dealing with cybersecurity.
	Being unable to sustain situational awareness among commanders and staff.	To plan cyber threat situational awareness training for commanders and staff to remind that cybersecurity is the commander responsibility.
To Defend Army Critical Information Systems Against cyber Attacks.	Enough workforce assignment of cyber professional and a clear definition of "defense, active defense and offense" in procedures.	To defend information systems 24/7.
		To hire part time or full time civilian contractors, engineers, hackers and malware analysts.
	Building strong coordination with intelligence organizations.	To assign liaison personnel mutually between cyber command and intelligence units.
The Risks of Open Source Intelligence (OSINT) and Social Networks.	Being an easy target to fishing attacks.	To plan cyber exercises to draw attention of leading cyber attacks (fishing, waterhole attacks, etc.)
	Gathering OSINT via social networks with masked and fake social network accounts.	To limit the use of social networks in military organizations.
	Using metadata of uploaded contents and EXIF information of uploaded photos [21]	To assign a content operator to control, erase and change the metadata and other information of contents.

3.2.2 Center of Gravity (COG) Analysis

Among the elements of cyber operational design, CCOG is the key one to reach the desired end state. In center of gravity analysis, there are several questions to be answered: What's the end state that the enemy wants? What kind of activities can the enemy perform to reach the end state? Which requirements support enemy's such activity? And which activities prevent the friend to achieve its end state? In CCOG analysis we can get the advantage of cyber factor analysis that consists of critical friend and enemy capabilities, missions and vulnerabilities.

3.2 Operational Art and Operational Design

3.2.1 Operational Art

According to Joint Pub 1-02, operational art is defined as the use of military forces to reach military objectives (strategic and operational) with design, organization, integration, and use of strategies. [24] Operational art plays a key role in conveying the commander's intuition and strategy into operational design by accounting all related factors of war.

Table 2: A Sample of Cyber Center of Gravity (CCOG) Analysis.

Cyber Center of Gravity (CCOG)	**Critical Capabilities (CC)**
SCADA Systems and Military Information Systems Infrastructure.	To implement cyber attacks against SCADA Systems by manual means (Hiring a person/supporter to use a malware/worm infected hard drive on these systems).
	To infect enemy's military information systems with a computer virus, worm or malware to steal or gather information (Screen shots, key strokes and files) by infiltrating into the systems or spear fishing by using social networks, open source intelligence (OSINT) and social engineering.
	To implement a zero day exploit to database, email, file servers that are connected on internet.
	To implement DDOS attacks.
	To implement cyber-electronic warfare activities in order to get electronic intelligence from frequency logs of command and control systems by using airborne warning/intelligence systems or drones.
Critical Vulnerabilities (CV)	**Critical Requirements (CR)**
Limited use of cyber intelligence activities.	To gather OSINT about SCADA/Cyber Physical Systems and their system requirements by using TOR networks or spoofed IP addresses.
National and international legal challenges and NATO perspective on cyber issues (Accepting it as an act of war or not, ambiguity of cyber rules of engagements etc.)	Preparing a legal frame document that clearly defines the activities, tasks and duties about cyber.
Lack of talented cyber specialists and cyber manpower planning in military organizations.	Reverse engineering and multi criteria analysis of some well known malwares directed to gather information from the systems they infected.
Lack of a roadmap and strategy designed to reach the national cyber security policy, lack of information sharing with institutions, universities and defense firms.	To initiate a collaboration and among technical universities, civil institutions and defense firms about research and development (R&D) in cyber
Lack of a clear task definition of cyber activities among institutions.	Forming a social network team, working 24/7 and solely focusing on Facebook, Twitter, LinkedIn, Vine, Instagram and the others also.
The lack of integration of cyber and intelligence units and the dilemma of whose job that is, limited cooperation between these two functional areas.	To have a national vulnerability database and enough cyber experts and contractors.
The legal challenges.	A great number of zombie computers, botnes.
The difficulty in integrating and implementing cyber and electromagnetic activities in tactical level under a command.	Strong cooperation between intelligence cyber units.

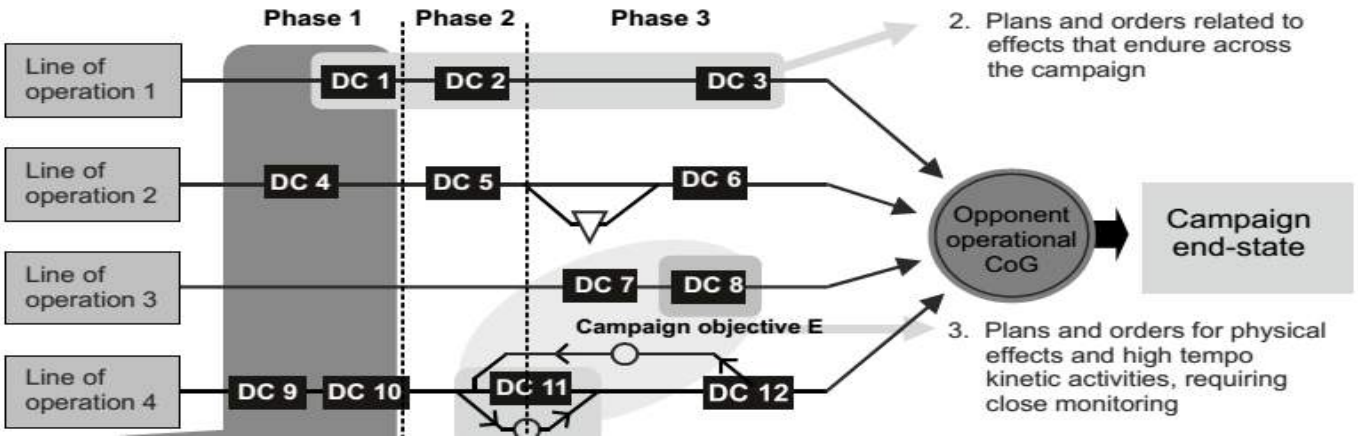


Figure 1: A sample cognitive map of an operational design [28]

3.2.2 Operational Design

Operational design is a methodology having the structure of concepts, a visual and comprehensive map of a campaign or operation in order to attain the desired end state. [25]. The main elements of operational design showed in figure 1are; line of operations (LOO), decisive points (DC), center of gravity (COG), end state are shown in a sample cognitive map of an operational design.

3.2.3 Critical and Creative Thinking

To deal with complex and multidimensional problems and develop solutions, operational designers should apply critical and creative thinking [15]. Critical thinking is a process comprising of conceptualizing, applying, analyzing, synthesizing, and/or evaluating information regardless of how it is gathered, produced, experienced or observed. [26]. While emphasizing on critical and creative thinking in operational design Bloom's Taxonomy of Learning can shed a light on this issue. As shown in figure 2, 1956 old model, developed for educational purposes, is a model that can help us relate critical thinking and creative thinking by associating them with the model's components [27] [15]. It is supposed that the commanders should be in a better level of their subordinates in creative thinking due to their experience, training and knowledge and judgement.

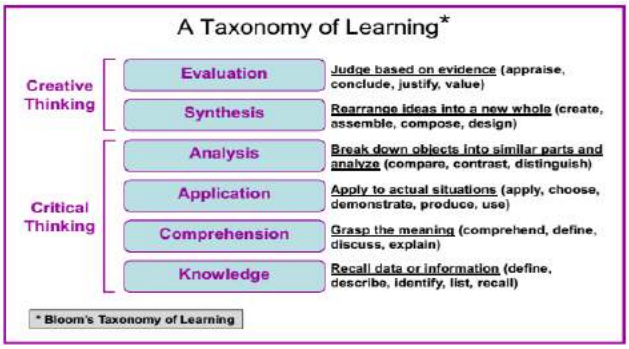


Figure 2: A taxonomy of learning [15].

4 CYBERSPACE OPERATIONS AND CYBER OPERATIONAL DESIGN

4.1 Cyberspace Operations (CO)

Cyberspace operations (CO) are the use of cyberspace capabilities where the main purpose is to attain the objectives in or through cyberspace [29]. With the advent of cyber in the globe theatre, it has become a must for commanders and operation planners to take necessary measures to protect their ICT and critical assets. In military operations, similar to electronic warfare planning and support of operations, CO should also be integrated into these operations according to its level. CO integration into military operations should be planned in detail by following the MDMP. The considerations of CO planners in MDMP are similar to other functional area considerations. With the start of MDMP, CO planners are going to need intelligence requirements about the enemy and environment.

Depending on the commander's intent or CO planners, cyber operational design should be prepared by CO planners before or with the first step of MDMP, receipt of mission. Having a cyber operational design will help CO planners to better integrate their objectives with major military operations.

4.2 Cyber Operational Design (COD)

The designing of cyber operations regardless of the common operation picture (COP) or not within an MDMP, may cause the expected impact become weak and ineffective. Eliciting the art of war and stimulating the critical and creative thinking, operational design put forward the general picture of operation, which is called the cognitive map.

In a cyber cognitive map, cyber operational design, the same elements of operational design are applied. Cyber operational design (COD) consists of cyber line of operations (Government, people and military), Decisive Points (DC), center of gravity (COG) and the end state (Desired End State). All elements of cyber operational design in figure 3 should serve to reach the end state in four phases of which starts with "Confusion Initiation" and ends with "Dominate" phase. The cyber operational design in figure 4 can also be adjusted to all levels of military or governmental organizations by elaborating more than one COG (Operational and Strategic COG) or End State (Military and Governmental End State).

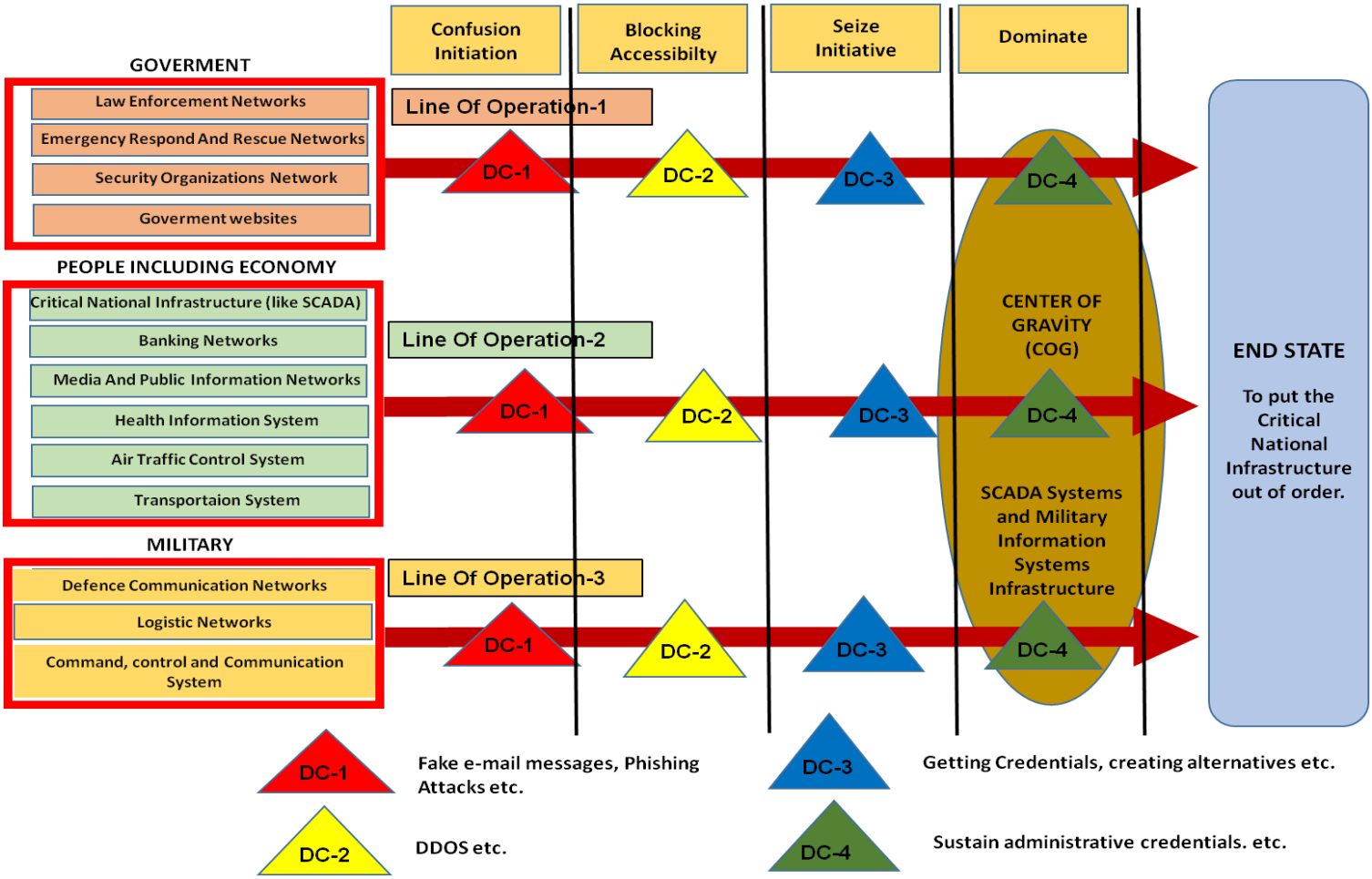


Figure 3: A Sample Cognitive Map of Cyber Operational Design.

5 CONCLUSION

In complex, multidimensional and multivariable security environment, it has become a must to get prepared all kinds of threats. What is becoming obvious that, with the evolving and cutting edge technology most of the threats are somehow emerging or being transferred with information systems. National Critical Infrastructures of countries are operating in networks, government and military organizations' data centers are working with software and hardware that even the system administrators can't control over them thoroughly. With the increasing use of smart devices, phones, appliances and even cars people become more and more interconnected with technology every day. Increasing use of social networks and all other improvements as a natural consequence of technological evolutions have facilitated the work of intelligence agents and cyber criminals. To gather information via open source and social networks like Facebook, twitter, LinkedIn, Instagram and the others have become an easy job even for a standard internet user. What the government and military organizations should do in this changing security environment is to scrutinize the current plans and procedures to support the flexibility of operations to adapt to new, unforeseen threats and risks that we sooner or later may be exposed to.

We assume that cyber incidents will continue to play a significant role in global theatre and institutions should be well prepared to withstand and defend their critical assets which are mostly on our networks, databases and command control systems. In this context, we make an analogy of ill-structured problems with cyber threats/attacks that are complicated, hard to detect and targeted. Therefore by emphasizing the importance of design and its elements, we propose a cyber operational design to be used in cyberspace operations to envision the cyber threats, cyber attacks, cyber intelligence and espionage activities both conceptually and comprehensively. We believe that by having a cyber operational design, the operation planners and cyber professionals will come to a common point where they can understand and contribute each other well and this cooperation will then provide a stronger, foreseeable institutional and national cybersecurity.

6 REFERENCES

[1]. Handel, M. I. (2005). *Masters of war: classical strategic thought*. Routledge.

[2]. Handel, M. I., (1991) Sun Tzu and Clausewitz: The Art of War and On War Compared, Strategic Studies Institute U.S. Army War College Carlisle Barracks, Pennsylvania.

[3]. Pamphlet, T. R. A. D. O. C. (2010). TRADOC Pamphlet Cyberspace Operations Concept Capability Plan2016-2028. Washington, DC: DoD.

[4]. Goztepe, K., Kilic, R., & Kayaalp, A. (2014). Cyber Defense In Depth: Designing Cyber Security Agency Organization For Turkey. Journal of Naval Science and Engineering, 10(1), 1-24.

[5]. Goztepe, K. (2012). Designing Fuzzy Rule Based Expert System for Cyber Security. International Journal of Information Security Science, 1(1), 13-19.

[6]. Singh, A. K., & Sahu, R. (2008). Integrating Internet, telephones, and call centers for delivering better quality e-governance to all citizens. Government Information Quarterly, 25(3), 477-490.

[7]. Güngör, V. C., Sahin, D., Kocak, T., Ergüt, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: communication technologies and standards. Industrial informatics, IEEE transactions on, 7(4), 529-539.

[8]. Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. Trends in organized crime, 11(3), 270-295

[9]. Kay M., J. (2014) "ISIS Tactics Illustrate Social Media's New Place In Modern War", [online], http://techcrunch.com/2014/10/15/isis-tactics-illustrate-social-medias-new-place-in-modern-war/

[10]. Boz, G. (2014) "ISIS and Social Media", [online], Ankara Strategy Institute, http://www.ankarastrateji.org/haber/isis-and-social-media-1399/

[11]. Newman, N., Dutton, W. H., & Blank, G. (2012). Social media in the changing ecology of news: The fourth and fifth estates in Britain. International Journal of Internet Science, 7(1), 6-22.

[12]. Hejase, A. J., Hejase, H. J., & Hejase, J. A. (2015) Cyber Warfare Awareness in Lebanon: Exploratory Research. International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(4): 482-497

[13]. Al-Ahmad, W. (2013). A Detailed Strategy for Managing Corporation Cyber War Security. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2(4), 1-9.

[14]. Liang, Q., & Xiangsui, W. (1999). Unrestricted warfare (pp. 551-563). Beijing: PLA Literature and Arts Publishing House.

[15]. Joint Staff, J-7 (2011) Planner's Handbook for Operational Design, Joint and Coalition Warfighting Suffolk, Virginia.

[16]. Lussier, J. W., Shadrick, S. B., & Prevou, M. I. (2003). Think Like a Commander prototype: Instructor's guide to adaptive thinking (No. ARI-RP-2003-02). Army Research Inst. for the Behavioral and Social Sciences Alexandria VA.

[17]. FM 5-0. (2010) The Operations Process, Headquarters Department of The Army.

[18]. FM 101-5. (1997) Staff Organization and Operations, Headquarters Department of the Army Washington, DC.

[19]. Kober, A.E. (2010) Bridging the Planning Gap: Linking Conceptual Army Design to Military Decision-Making, School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas.

[20]. Grigsby Jr, W. W., Gorman, S., Marr, J., McLamb, J., Stewart, M., & Schifferle, P. (2012). Integrated Planning the Operations Process, Design, and the Military Decision Making Process. Military Review, 92(4), 15.

[21]. Catalkaya H., Karaman M. (2015). Institutional Cybersecurity: The Risk of Open Source Intelligence (OSINT) and Social Networks, International Conference on Military Security Studies (ICMSS-2015), Istanbul.

[22]. Kem J.D. (2012) Planning for Action: Campaign Concepts and Tools, U.S. Army Command and General Staff College U.S. Army Combined Arms Center Fort Leavenworth, Kansas.

[23]. Goztepe, K., Kahraman, C. (2015) A New Approach to Military Decision Making Process: Suggestions from MCDM Point of View, International Conference on Military and Security Studies-2015, Istanbul, 118-122.

[24]. Joint Publication 1-02 (1994) Department of Defense Dictionary of Military and Associated Terms, Headquarters Department of Defense.

[25]. McCauley, D. (2011). Design and Joint Operation Planning. Canadian Military Journal, 12(1), 30-40.

[26]. Scriven M., Paul R. (1987) "National Council for Excellence in Critical Thinking", 8th Annual International Conference on Critical Thinking and Education Reform, Summer 1987.

[27]. Bloom, B., & Englehart, M. F. E., Hill, W., & Krathwohl, D.(1956). Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain.

[28]. Joint Publication 5-0 (2011) Joint Operation Planning, Headquarters Department of Defense.

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(1): 30-45
The Society of Digital Information and Wireless Communications, 2016 (ISSN: 2305-0012)

Enhancing AES using Novel Block Key Generation Algorithm and Key Dependent S-boxes

Harpreet Singh, Paramvir Singh
Department of Computer Science and Engineering
Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India
singh.harpreet89@hotmail.com, singhpv@nitj.ac.in

ABSTRACT

Security is one of the vital aspects of data communication, a wide acceptance of AES shows its superiority in providing confidentiality to secret information. Several algorithms have been proposed in recent times to modify the static nature of S-boxes used in AES. All these algorithms use same secret key to encrypt each plain text block. This paper presents a novel Block key generation algorithm in synchrony with dynamic S-box generation algorithm to generate considerably more unpredictable cipher texts in comparison to existing dynamic S-box generation techniques. Each plain text block is encrypted using entirely different block key generated from the secret key, which in turn generates non identical S-boxes to encrypt each plain text block. The proposed algorithm revamps the cryptographic strength of original AES by eliminating any possibility of cryptanalysis, and is both reliable and easy to implement.

KEYWORDS

Cryptographic algorithms, AES, Block cipher, Block key generation, S-box, Key dependend S-box, Modes of Operation, Dynamic S-box

1 INTRODUCTION

In the modern era of technological advancements numerous communication channels are being vastly used for transmission of colossal amount of classified data. Information related to application areas such as military and business transactions are confidential or private, hence cannot be compromised at any cost. Various cryptographic techniques are widely in use for encrypting data to be transmitted over unsecured channels. Even though cryptographic algorithms assure security, warranting security has become more and more challenging as innumerable communication channels are arbitrated by attackers [5]. The number of end users utilizing unsecured communication channels are growing exponentially with the passage of each day. Moreover, multitudinous of experiments are being actively conducted all around the world to check the feasibility of upcoming block ciphers against different known attacks. On the other hand, some researchers are constantly enhancing already available block ciphers either by reducing their time, space complexities or by making them resilient to myriad of upcoming attacks.

The choice of using an encryption algorithm purely depends on the amount of data to be encrypted and the requirements of the parties involved. Mainly there are two categories of encryption algorithms known as symmetric key algorithms and asymmetric key algorithms. *Symmetric key* algorithms are more suitable for encrypting enormous amounts of data, therefore most commonly used algorithms including Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES) use a secret key for the purpose of encryption and decryption. However, *Asymmetric key* algorithms like Rivest-Shamir-Adleman (RSA) and Elliptic Curve Algorithms (ECA) are most commonly used to mutate petty amounts of data, and utilize private and public key pairs for encryption and decryption.

Modern block ciphers are based on symmetric key cryptography and transform 128 or 256 bits of plain text into similar lengths of cipher text bits by utilizing 128, 192 or 256 bits secret key. Each block cipher is based on a combination of two universal principles, Confusion and Diffusion. *Diffusion* is responsible for dispersing the effect of a single plain text bit to numerous cipher text bits, which means that a single change in the plain text

character leads to entirely different cipher text. It also hides the relationship between plain text and cipher text [30], which in turn, makes statistical attacks almost impossible. On the other hand, *Confusion* creates a complex relation between plain text and secret key, where every bit of cipher text depends on many secret key bits. In other words, a single bit change in the secret key generates entirely different cipher text [28]. Consequently, finding the secret key from cipher text is not feasible.

This paper introduces an ingenious algorithm which is used in simultaneity with key dependent AES to encrypt plain text blocks with discrete block keys. The round keys used in AES implementation depends on the secret key provided by the user, but the proposed algorithm utilizes non-identical block keys which in turn generates different round keys for the purpose of encryption and decryption of each plain text or cipher text block. Further, dissimilar S-boxes are created by employing different rounds keys to be used in *Substitute Bytes* and *Add Round Key* transformations. Besides that, this paper also evaluates the proposed algorithm on the basis of operational complexity and avalanche effect in contrast to AES used in conjunction with ECB or CBC mode.

The structure of this paper is as follows: Section 2 presents a brief introduction about primitive AES and commonly used Modes of operation used in synchronicity with block ciphers. Section 3 describes the related work that has been conducted to increase the strength of AES over the years. Proposed encryption algorithm is explained in Section 4. Experimental setup is described in Section 5. Results and analysis are presented in Section 6 followed by Section 7 that concludes the paper.

2 ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) was specifically designed to replace the aging Data Encryption Standard, Its selection procedure begun back in January 2, 1997 by National Institute of Standards and Technology (NIST) of the United States of America [1] [2] when they summoned world's finest minds in the field of cryptography to cooperate by presenting their ideas for a new encryption algorithm to be called as Advanced Encryption Standard and succeeded in its agenda with the submission of 15 algorithms as potential candidates for AES. NIST has also intended to make all the submissions available to public for their valuable comments and reviews. After initial assessments five new algorithms (MARS, RC6, Twofish, Serpent, and Rijndael) have been selected as AES finalists, following innumerable reviews and public scrutiny, Federal Information Processing Standard (FIPS) published the draft for Advanced Encryption Standard in February 28, 2001 and final AES was approved on November 26, 2001 as FIPS PUB 197 [3].

Advanced Encryption Standard (AES) formally known as Rijndael is an algorithm that belongs to the family of Block ciphers and was proposed by Joan Daemen and Vincent Rijmen [1]. It does not use Fiestel structure like Data Encryption Standard (DES) where 32 out of 64 bits are encrypted in each round. Instead, AES encrypt all 128 bits of plain text in a single round, which is the reason of its lower number of rounds as compared to DES [27]. However, in addition to AES design criteria, actual Rijndael algorithm has the capability to encrypt 192 or 256 bits of plain text using 128, 192 or 256 bits of secret keys respectively.

2.1 Basic AES

AES encrypts a block of 16 bytes of plain text into 16 bytes of cipher text and is designed to use variable key sizes of 16, 24 or 32 bytes respectively, depending on user requirements. Hence, precisely 16 * 8 = 128 bits of plain text is used as input and 16 * 8 = 128 bits of cipher text is generated as output. Likewise, any of 128, 192 or 256 bits of keys can be used in encryption process.

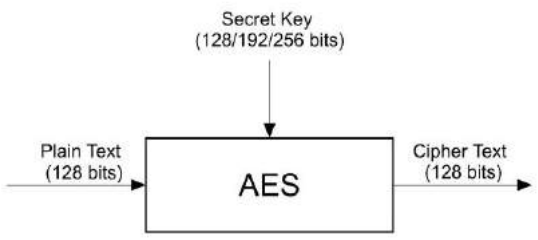


Figure 1. High level block diagram of AES

Number of rounds in AES depends upon the key size. If key size is 128/192/256 bits, then number of rounds (Nr) are 10/12/14 respectively [29].

Table 1. Parameters of three AES variants

	AES – 128	AES - 192	AES - 256
Plain Text Length	128 bits	128 bits	128 bits
Cipher Text Length	128 bits	128 bits	128 bits
Key Length	128 bits	192 bits	256 bits
Round key Length	128 bits	192 bits	256 bits
Number of Rounds	10	12	14

AES is a byte oriented encryption algorithm consisting 10 rounds, where each round comprises four different types of transformations. These transformations collaborate to mutate 16 bytes of State Array. A *State Array* is nothing but a matrix organization of bytes in 4 * 4 form. Initially, State Array contains the plain text to be encrypted, which evolves toward becoming the cipher text with the passage of each round.

The process of encrypting each block (i.e. 16 bytes) in AES-128 variant begins with the initiation of *Round Key Generation*, formally known as *Key Expansion Routine*, where secret key undergoes a series of transmutations based on substitution, rotation and round constants to generate a linear array holding 176 bytes (i.e. 11, 16 byte round keys). On the other hand, *Round Key Generation* for AES-192 and AES-256 generates a linear array of 208 bytes and 240 bytes respectively.

Actual encryption of AES-128 variant initiates with round 0, also known as 'Input Whitening' which contains only an *Add Round key* operation and it consumes first 16 bytes of the round key. This is followed by 9 rounds comprising *Substitute Bytes, Shift Rows, Mix Columns* and *Add Round Key*. Further, it is important to note that *Add Round Key* utilizes next 144 bytes of round key over the span of these 9 rounds, while *Mix Columns* is omitted from the 10th round and *Add Round Key* operation uses remaining 16 bytes of round key.

Figure 2 shows encryption and decryption steps of AES.

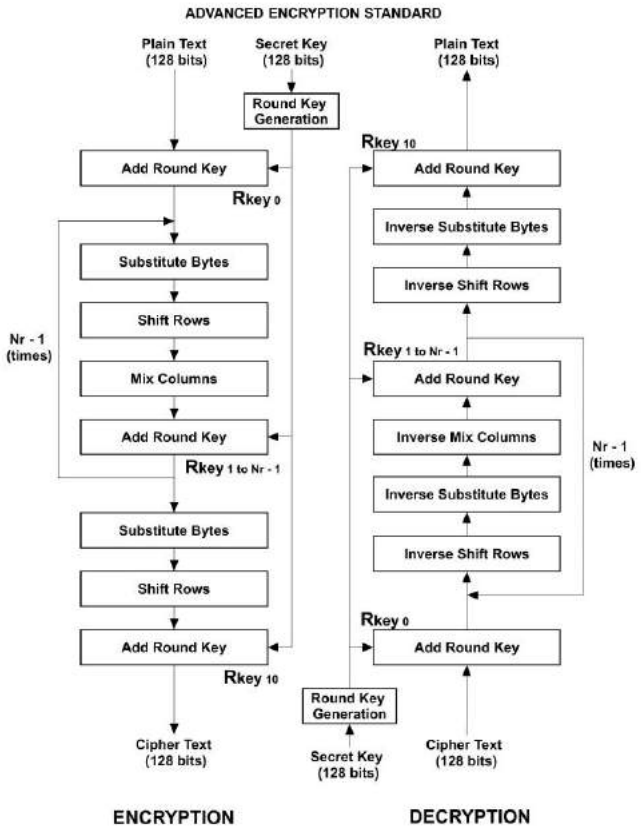


Figure 2. Encryption and Decryption of AES

(i) Add Round Key

This involves a simple XOR operation between *State Array* of 128 bits (16 bytes) and *Round Key* of 128 bits (16 bytes).

(ii) Substitute Bytes Transformation

This includes substitution of *State Array* bytes according to a 16 * 16 substitution table (S-box) having 256 different values. S-box is constructed by calculating the multiplicative inverse of each byte ranging between 00 to FF in hexadecimal form, and is followed by an affine transformation. This is a nonlinear byte substitution and provides strong *Confusion* [5].

(iii) Shift Rows Transformation

A row wise transposition operation is applied on the bytes of *State Array*. First row remains the same. Second row is cyclically shifted by one byte to the left. Third row is cyclically shifted by two bytes to the left and Fourth row is cyclically shifted by three bytes to the left.

(iv) Mix Columns Transformation

This transformation treats the *State Array* column as a four term polynomial and a fixed matrix is multiplied by each column using Galois field [2].

Shift Rows and *Mix Columns* provide *Diffusion,* while *Substitute Bytes* and *Add Round Key* dispense *Confusion* in case of AES. The only nonlinear part of AES is its static S-boxes which in turn makes AES susceptible to linear and differential cryptanalysis.

S-boxes used for "encryption" and "decryption" are depicted in Figure 3 and Figure 4 respectively [32].

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 3. S-box used in Encryption

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Figure 4. Inverse S-box used in Decryption

2.2 Modes of Operation

An algorithm used in conjunction with block ciphers to provide authenticity and confidentiality is referred as a mode of operation [31]. A block cipher is capable of securely transforming only a fixed block of plain text [24]. Consequently, a mode of operation is used to repeatedly apply block cipher algorithm to encrypt plain texts larger than a single block (i.e. 128 bit in case of AES). Two of the most popularly used modes of operation for block ciphers are Electronic Codebook (ECB) and Cipher Block Chaining (CBC).

(i) Electronic Codebook (ECB)

Each plain text is encrypted independently and the output of one block does not affect the output of any other block. Usage of ECB is usually discouraged because: it does not hide data patterns, resulting in the generation of identical cipher texts from similar plain texts.

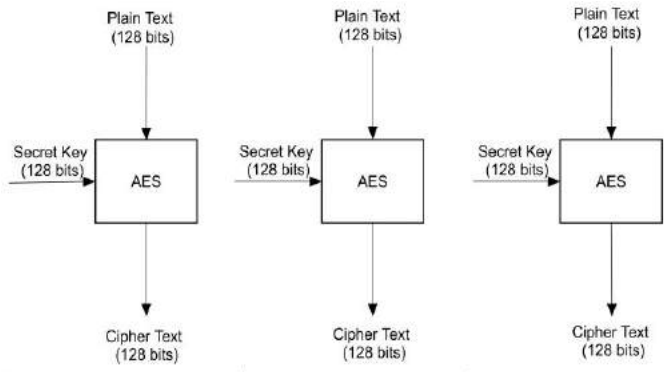


Figure 5. Electronic Codebook

However, all plain text blocks can be encrypted in parallel by using Electronic Codebook (ECB).

(ii) Cipher Block Chaining (CBC)

Each plain text encryption depends upon the cipher text of the previous block with only one exception that the output of first plain text block depends on Initial Vector (IV) which can be generated by any of the FIPS recommended Cryptographically Random Number Generators (PRNG's) [25].

CBC mode eliminates the disadvantage of ECB by perfectly hiding plain text patterns resulting in the generation of non-identical cipher texts from

similar plain texts, however, it lacks parallelizable encryption.

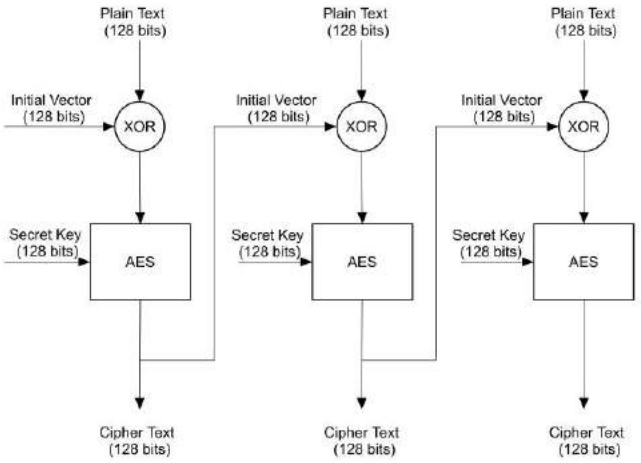


Figure 6. Cipher Block Chaining

3 RELATED WORK

Over the last one decade, many researchers have come up with new techniques to enhance the security of Advanced Encryption Standard (AES) with the help of key dependent S-boxes. A brief analysis depicting the analysis and proposed modifications are defined in this Section.

Webster and Tavares [26] explained that a cryptographic transformation exhibits the property of completeness only if each of the cipher text bit depends on all the plain text bits. Thus, if there exists a *Boolean* expression, and it represents each cipher text in terms on plain text bits is complete, only if it contains all of the plain text bits. They further explained that in order to exhibit Strict avalanche criterion, the output bits should change with the probability of one half when a single bit of plain text is altered. In addition, a second property that every cryptographic transform should have is the pairwise independence between all of the avalanche variables which can be calculated with the help of correlation coefficients. Furthermore, these transforms should also possess the property of invertibility.

Ferguson et al. [13] demonstrated that the algebraic formulae of AES is simpler than the other known block ciphers. They further concluded that the security of AES purely depends on the infeasibility of solving its algebraic expression and it is probable to broken in the upcoming years. But, at the moment it is computationally secure and can be confidently used in security critical applications.

Nejad et al. [8] compared the avalanche effect and simulation times of both primitive AES and AES with key dependent S-boxes. They further concluded that AES with key dependent S-boxes rectifies the fixed structure problem of normal AES with an additional property of higher avalanche effect. As, the higher avalanche effect leads to enhancing the level of security which in turn justifies the extra time taken to implement dynamic S-boxes.

Gupta and Sarkar [10] presented two new techniques to generate non-linear resilient S-boxes and proved that the correlation immunity of the resilient S-boxes is preserved under composition with an arbitrary Boolean function. However, their techniques were not resistant to the algebraic attacks.

Fahmy et al. [12] introduced a new technique to generate key dependent S-box especially for AES, which can be generated from the secret key with the help of two linear congruence parameters of ISO-C Standard and GNU-C respectively. They further tested their algorithm for measuring randomness and found satisfactory results. But, their technique has completely replaced original S-box with new dynamic S-box and eliminated the Inverse S-box, which is the complete violation of AES design.

Krishnamurthy and Ramaswami [6] came up with a new idea to modify the original structure of AES with an inclusion of one additional state named as *Rotate S-box* at the beginning of each round, while decryption had only four states where Inverse *Substitute Bytes* were tweaked to nullify the effect of *Rotate S-box* state used in encryption. They successfully depicted that the extra time required for an extra state and tweaked *Inverse Substitute Bytes* is negligible and their algorithm is immune to cryptanalysis.

Kazlauskas and Kazlauskas [9] have proposed a new algorithm which is capable of generating a key dependent S-box to avoid linear and differential cryptanalysis due to static S-box. They have also introduced a modification in *Key Scheduling* algorithm, where substitution of bytes is omitted from the round keys generation. In addition, they have shown that independency measure ratio of S-box generated by their algorithm is roughly identical to model ratio for independent and individual numbers. Moreover, main advantage of their approach is to be able to generate numerous S-boxes by changing the secret key. However, the proposed algorithm consumes significant amount of time to generate dynamic S-boxes.

Stoinov [16] has proposed a new design where four different S-boxes could be used in the encryption process. He used both original S-box, and original Inverse S-box to generate two additional S-boxes on the basis of taking left and right diagonals as axis of symmetry followed by changing the location of corresponding bytes. Moreover, he has successfully tested newly generated S-boxes for balancing, non-linearity, strict avalanche criterion, low XOR table, diffusion order, invertability, and concluded that all four S-boxes could be used for encryption and their Inverse S-boxes could be used for decryption without compromising the security. The actual downside of this design is to use pre calculated S-boxes, which do not depend directly upon the secret key or round keys.

Gong et al. [21] proposed a new AES implementation on the basis of five lookup tables generated from original S-box. The advantages include reduction in the code-size in comparison to original AES and improvement in efficiency of implementation. Although, this new design is significantly proficient on FPGA devices, yet it contradicts primitive structure of AES and is not tested against any of the statistical tests.

Isa et al. [20] reviewed existing attacks on the AES and successfully analyzed the efficiency of recent block cipher proposals as alternatives to the key scheduling algorithm of basic AES which can withstand known attacks. Furthermore, they have compared different modified key schedule algorithms for AES to counter single key and related key attacks, and concluded that security of AES is still intact as these attacks are still theoretical in nature.

Juremi et al. [11] have designed a new AES like design for key dependent S-boxes using rotation. They carefully manifested how the property of S-box rotation can be used to create key dependent S-boxes from round keys. The cipher structure of proposed algorithm resembles original AES and with an addition of key dependent S-box without changing its values. Further, modified AES algorithm does not contradict the security and design parameters of original AES, as all of the mathematical criteria were kept unchanged.

Sahoo et al. [19] have proposed to utilize a different affine transformation in the creation of static S-boxes to be used in encryption and decryption. Implementation time has been calculated experimentally for S-box generation using standard and newly proposed affine transformation. It has been deduced that time taken to generate the S-box is slight improved. But, no attention has been paid to test the proposal against any of the security metrics. Consequently, minute advantage in execution time cannot neutralize lack in cryptographic strength.

Pradeep and Bhattacharjya [22] have proposed an approach to generate random session keys from the master key (secret key) provided by the user in conjunction with dynamic S-box generation algorithm. The proposed algorithm is immune to cryptanalysis. Further, the purpose of using non-identical session keys is to encrypt each block using dissimilar keys to overcome the likelihood of brute force attacks.

Nadaf and Desai [7] proposed a new algorithm which is able to generate key dependent S-boxes and is also optimized to run on FPGA devices. The proposed algorithm does not contradict any design property and is able to encrypt faster on the hardware with resilience to linear and differential cryptanalysis.

Abhiram et al. [15] have modified the basic structure of AES by harnessing dual round keys, generated from the secret key. Proposed algorithm further tweaks *Shift Rows* by making it key dependent with an inclusion of new transformation referred as *Shift columns*. One of the two round keys are used in *Substitute Bytes* and *Shift Columns* transformation. While the second key is employed in *Shift Rows* and *Add Round Key* transformation. Further, they have demonstrated that the modified algorithm can easily be implemented on FPGA devices and intensifies the complexity of brute force attack in comparison to the standard AES.

Felicisimo V. Wenceslao, Jr [18] has completely revamped AES with the use of multiple S-boxes to replace *Mix Columns* transformation with a novel *Substitute Bytes XOR* transformation. They have further shown that the efficiency of encryption has been enhanced and the efficiency of decryption has been degraded in comparison to basic AES. But, at the same time avalanche effect has been plummeted to below acceptance rates for the samples differ by one bit.

Jacob et al. [5] have revealed a new method to generate dynamic S-boxes based on a *codeword* generated from the secret key by calculating hamming distance and hamming weight of certain key bits with the properties of bijection, strict avalanche criterion, correlation immunity, non-linearity and balance. They have thoroughly displayed that their algorithm is simple, easy to implement, very difficult to guess and is immune to linear and differential cryptanalysis.

Kazlauskas et al. [14] have proposed another algorithm to generate key dependent S-box and have successfully scrutinized their algorithm for randomness. Further experimental results proved that cipher text sequences generated are random. Also the sequences that have been generated were in proximity with the number of ones and zeroes in true random sequence. Furthermore, proposed algorithm is resistant to linear and differential cryptanalysis and is faster in terms of execution speed in comparison to the one described in the paper by Kazlauskas and Kazlauskas [9].

The utilization of dynamic S-boxes is one of the main strength of any cipher system, since both linear and differential cryptanalysis require the known S-boxes [14]. So, researchers have mainly focused on the techniques to amend the static nature of S-boxes being used in AES.

Najaftorkaman and Kazazi [23] have studied the DNA-based cryptography and proposed a novel encryption technique to encrypt binary data. They have further evaluated the validity of their algorithm using probability theory and the DNA strant properties.

The above mentioned work clearly manifests that till date, AES has not been modified in light of hiding plain text patterns together with providing parallel encryption. (i.e. providing advantages of both ECB and CBC modes). The prime objective of proposed algorithm presented in Section 4 is to transform AES in order to implement parallel encryption and decryption while disguising plain text patterns. Further, the inclusion of key dependent S-boxes neutralizes any threat of linear and differential cryptanalysis.

4 PROPOSED ALGORITHM

Primitive Advanced Encryption Standard (AES) briefed in the Section 2 uses static S-boxes in each round and a user defined secret key to encrypt each block of plain text. That is if the length of plain text is 256 bits, then it will be divided into two 128 bit blocks. Each of them is encrypted using the same secret key and any of the modes of operation.

On the other hand, this newly proposed approach uses an innovative Block key generation algorithm with an addition of dynamic S-box generation algorithm. This new design can be applied to AES-128 variant, where secret key is 128 bits long. All of the block keys are generated prior to the inception of Advanced Encryption Standard (AES), this property makes it possible to encrypt each block of plain text in parallel and hide plain text patterns.

Encryption and decryption using Block key generation algorithm is shown in Figure 7.

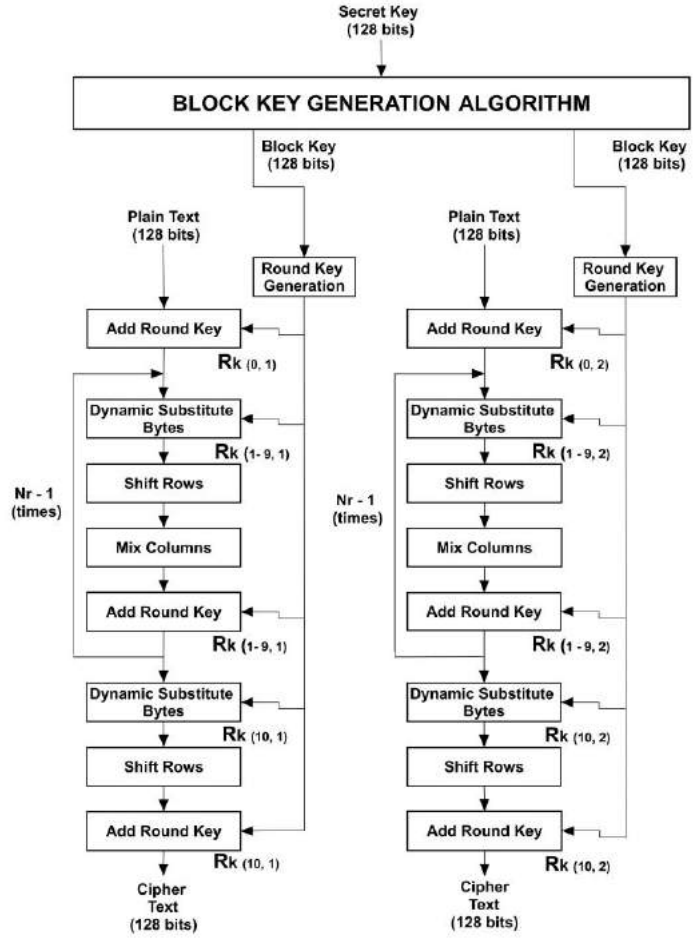


Figure 7. Encryption using Block Key Generation Algorithm with Dynamic S-boxes

The proposed Block key generation algorithm and key dependent S-box generation are described in the following subsections.

4.1 Block Key Generation Algorithm (BKG)

Block key generation algorithm (BKG) generates non identical block keys from the user provided secret key to encrypt every block of plain text.

Initially, the secret key is rearranged by the Permutation function. After than an exclusive OR operation amalgamate the output of permutation function with secret key. Now this transformed key acts as the input for SHA-256 algorithm and finally a Trimmed output creator creates 128 bit, block key to be used in encryption or decryption.

The process of generating block keys from the secret key is depicted in Figure 8.

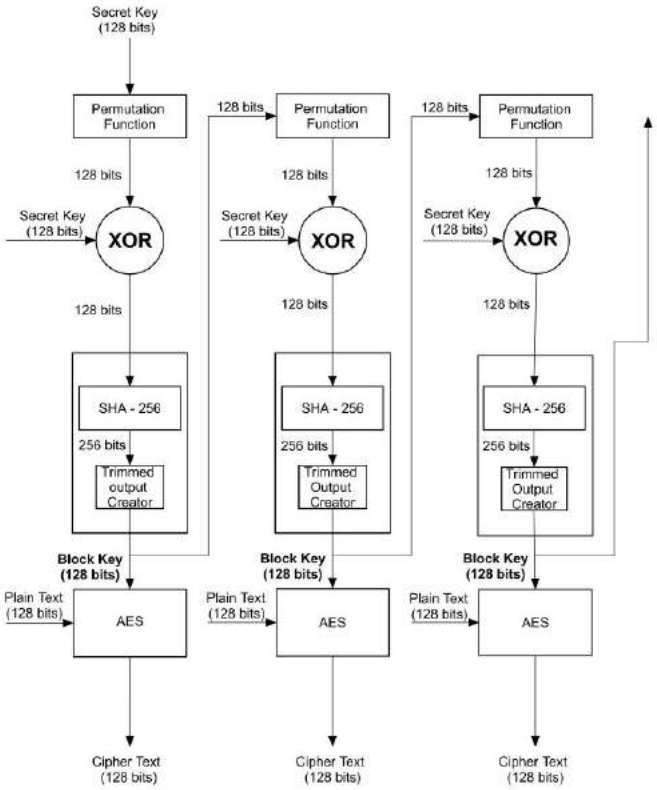


Figure 8. Block Key Generation Algorithm

(i) Permutation Function

This function takes 16 bytes (128 bits) of input. Firstly, it divides the input into two 8 bytes (64 bits) left and right halves as shown in Figure 9.

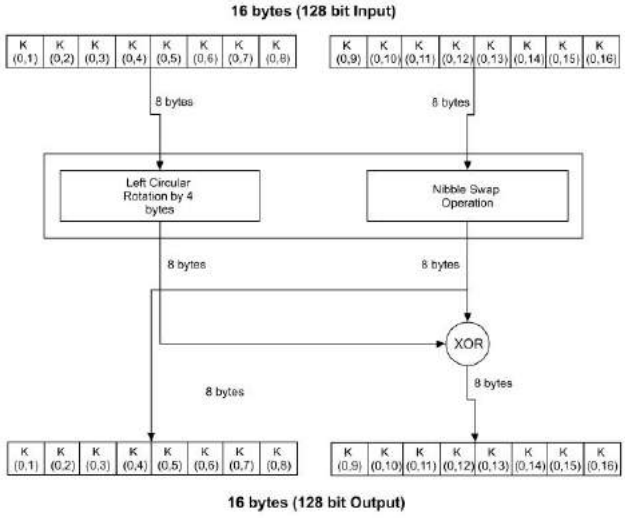


Figure 9. Permutation Function

Then, left half is cyclically rotated by 4 bytes to the left and Nibble swap operation (i.e. a4 becomes 4a) is performed on each byte of right half. In the

next step, the Nibble swapped right block becomes new left block and XOR operation is performed between Nibble swapped right block and cyclically rotated left block to create the new right block.

(ii) XOR
It is a simple exclusive OR operation between secret key and output generated by Permutation Function.

(iii) SHA-256
Secured hash algorithm is used to generate the hash of output generated in the previous step by XOR operation. Hashing is a one-way function where it is computationally not feasible to get back to the original message from the message digest [4].

(iv) Trimmed Output Creator
This is used to make the output generated by Secured hash algorithm (SHA-256) to 128 bits so that it can act as the block key for a given block. Firstly, the output of SHA-256 is divided into two 128 bit left and right parts, then a simple exclusive OR operation is applied to unify both parts as 128 bits output.

4.2 Key Dependent S-box Generation

Advanced Encryption standard uses static S-box for encryption generated by calculating multiple Inverse of each byte ranging between 00 to FF in hexadecimal form, and is followed by an affine transformation. While S-box used in decryption is inverse of that used in encryption. The process of encryption starts with a transformation known as *Add Round Key* of round 0 where secret key is used for "Input Whitening". Besides that, the secret key is also used to generate round keys prior to the execution of AES and are used in Round 1 to 10.

On the other hand, in key dependent S-box generation, a dynamic S-box is generated for each round by utilizing circular rotation of static S-box. Rotation is based on the round key and maps each byte of intermediate *State Array* into another byte trough S-box table lookup [9]. There are three simple steps to calculate dynamic S-box [17]:

- Get the Nr (round key)
- Apply XOR operation on every byte of round key.
  K1+K2+K3+K4+K5+K6+K7+K8+K9+K10+K11+K12+K13+K14+K15+K16
  Where, K1 to K16 are the bytes of round key.
- Resultant value is used for left circular rotation of static S-box.

Let us suppose that round key value for a particular round in hexadecimal form is:

c9 40 32 2b f2 43 cc e9 8b 29 0e a6 14 17 6c 3d

After applying XOR operation on the round key, resultant value generated is 5c in hexadecimal or 92 in decimal. Now the decimal value is used to cyclically rotate static S-box to the left by 92 bytes. The S-box shown in Figure 10 is generated after 92 bytes of cyclic rotations of static S-box to the left.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e5	f
0	4a	4c	58	cf	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f
1	50	3c	9f	a8	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21
2	10	ff	f3	d2	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d
3	64	5d	19	73	60	81	4f	dc	22	2a	90	88	46	ee	b8	14
4	de	5e	0b	db	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62
5	91	95	e4	79	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea
6	65	7a	ae	08	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f
7	4b	bd	8b	8a	70	3e	b5	66	48	03	f6	0e	61	35	57	b9
8	86	c1	1d	9e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9
9	ce	55	28	df	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f
a	b0	54	bb	16	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b
b	fe	d7	ab	76	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af
c	9c	a4	72	c0	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1
d	71	d8	31	15	04	c7	23	c3	18	96	5	9a	07	12	80	e2
e	eb	27	b2	75	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3
f	29	e3	2f	84	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39

Figure 10. Dynamic S-box dependent on round key

User can also choose a right circular operation to generate dynamic S-boxes.

A total of ten rotated S-boxes are used to encrypt 128 bits of plain text block while using a 128 bits key. These S-boxes are generated from the round keys which are further derived from the secret key by applying *Round key generation* algorithm prior to the block encryption.

5 EXPERIMENTAL SETUP

This section explains about the testing samples, implementation environment, methodology and comparison metrics used to execute the original and proposed algorithm.

5.1 Samples

A set of random numbers used in data science and cryptography are pseudo random numbers. They can be generated with the help of Pseudo Random Number Generators (PRNG) or Cryptographically Secured Pseudo Random Number Generators (CSPRNG) [34]. These types of algorithms use some mathematical techniques to generate a sequence of random numbers and are advantageous because of their high speed. However, a predominant flaw in these types of randomly generated numbers is that they tend to repeat the same sequence and are quite predictable. Innumerable modern CSPRNGs use a long repetition period and can be used to check the quality of an Encryption algorithm or a Hash function [34].

On the other hand, True Random Numbers generators (TRNG) use some kind of physical phenomenon, such as random mouse movements, amount of time between pressing different key strokes on a keyboard, decay of a radioactive source and atmospheric noise [34]. One of the major limitations of TRNG is their slow speed of random number generation. But, they are nondeterministic, meaning that the sequence of random numbers generated once cannot be produced again. So, TRNGs are preferred over PRNGs in the fields of data science and cryptography. The plain text samples used for testing have been generated by utilizing True Random Number Generator using atmospheric noise [33].

5.2 Implementation Environment

Software tools and platform used to implement original AES in conjunction with ECB and CBC mode along with the proposed algorithm are presented in Table 2.

Table 2. Tools and Platform Used

IDE	Eclipse Luna
Programing language	Java
JDK Version	1.8
Operating System	Windows 10 Pro 64-bit
Processor	Intel Core I7 3rd Gen, 2.4 Ghz
RAM	8.00 GB, 1600 Mhz
Graphics	2.00 GB, Nvidia Geforce 650M

5.3 Operational Complexity

To measure the efficiency (speed) of the proposed algorithm, operational complexity is used as one of the metrics. The operations used in AES include XOR, rotation, multiplication and table lookup. Let the cost of performing XOR operation be same as rotation and are denoted as O; further multiplication be denoted as M; and table lookup as L [20].

Additionally, the proposed AES using Block key generation algorithm and key dependent S-boxes encompass two additional operations: Nibble Swap and SHA-256, and are denoted by N and H respectively.

5.4 Avalanche Effect

Avalanche effect is an important characteristic for any encryption algorithm. This property can be observed by generating a cipher text from plain text followed by changing one bit of that plain text to generate the second cipher text accompanied by the number of bits changed in the outcome of two cipher texts.

$$\text{Avalanche Effect} = nb / tb \quad (1)$$

Where, nb = number of bits flipped in cipher text and tb = total bits of cipher text.

Total number of bits of cipher text in case of AES-128 variant are always 128.

The purpose of Avalanche effect test is to find out the number of cipher text bits changed if input is changed by one bit. A large change in the

cipher text bits indicates high avalanche Effect. If observed avalanche effect is high, then it would be harder to perform analysis on cipher text.

5.5 Methodology

Initially, a *True Random Number Generator* is utilized to generate a test sample followed by *Plain Text Set Generator*, where two plain text samples are created from the original sample.

Both plain texts differ by 1 bit. For instance, if first plain text block is:
09 15 c4 46 f9 82 7f f0 14 b5 25 19 31 27 03 60

Then, second plain text block could be:
09 15 c4 46 f9 82 7f f0 14 b5 25 19 31 27 03 61

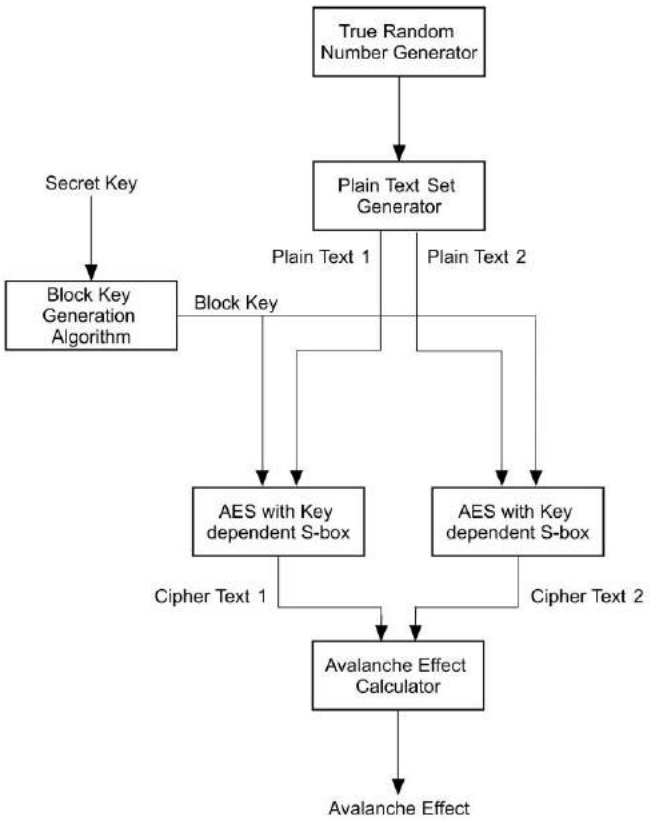


Figure 11. Experimental Methodology

Further procedure involves the generation of a block key from the secret key by employing a novel Block key generation algorithm. In the subsequent step, a modified Advanced Encryption Algorithm (i.e. AES with key dependent S-boxes) encrypt both of the plain text blocks to generate two cipher texts. Final step concludes with the calculation of avalanche effect according to the formulae defined in previous Subsection.

In addition, operational complexity can be calculated manually. It includes the procedure of counting different types of operations involved in the proposed algorithm and original AES when coupled with ECB or CBC mode.

6 RESULTS AND ANALYSIS

6.1 Operational Complexity Calculation

AES-128 requires 10 round keys to be generated from secret key. Each *Round Key Generation* includes 1 rotation (1O), 4 table lookups (4L) and 20 XOR (20O) operations. So, operational complexity for generating one round key is: 21O, 4L. Consequently, 10 round keys will consume 210O, 40L operations [20].

Moreover, each rounds of primitive AES comprises 16 table lookups (16L) in *Substitute Bytes*, 6 rotations (6O) *in Shift Rows*, 4 * 4 = 16 multiplications (16M) with 4 * 3 = 12 XORs (12O) in *Mix Columns* and 16 XORs in *Add Round Key* transformations. Thus, operational complexity of each round is 34O, 16M and 16L [20]. Hence, 10 rounds of encryption including initial *Input Whitening* round utilize 344O, 144M and 160L. Another key point to remember while calculating operational complexity is that *Mix columns* transformation is omitted from 10^{th} round.

Thus, operation complexity of each block of plain text encryption using AES in ECB mode is calculated by adding operational complexity of *Key Generation* algorithm and operational complexity of AES encryption. After successful addition total operational complexity of AES in ECB mode is: 554O, 144M, 200L.

On the other hand, CBC mode includes a XOR operation between Initial Vector (IV) and first plain text block before the inception of encryption algorithm. In addition, subsequent blocks consume

cipher text generated by previous block to perform XOR operation with plain text block. So, CBC mode requires 16 additional XOR operations (16O) in comparison to ECB mode.

Consequently, operation complexity of each block of plain text encryption using AES in CBC mode is calculated by adding operational complexity of AES in ECB mode and operational complexity of performing 16 supplementary XOR operations. After successful addition total operational complexity of AES in CBC mode is: 570O, 144M, 200L.

Whereas, BKG involves 4 Rotations (4O), 8 Nibble swaps (8N), 8 XOR (8O) operations in *Permutation Function*, 16 XOR (16O) operations to merge secret key and the output of *Permutation Function*, 1 hashing (1H) operation to generate SHA-256 digest and 16 XOR (16O) operations in *Trimmed Output Generator*. This implies that BKG requires additional 44O, 8N and 1H operations in comparison to ECB mode.

Therefore, operation complexity of each block of plain text encryption using AES with BKG is calculated by adding operational complexity of AES in ECB mode and operational complexity of BKG. After successful addition total operational complexity of AES with BKG is: 598O, 144M, 200L, 8N, 1H.

Table 3. Operational Complexities without key dependent S-boxes

Algorithm	Operational Complexity Parameters				
	O	M	L	N	H
AES with ECB Mode	554	144	200	0	0
AES with CBC Mode	570	144	200	0	0
AES with BKG	**598**	**144**	**200**	**8**	**1**

Key dependent S-box generation involves 15 XOR (15O) operations on each round key for the purpose of generating a rotation value. In addition, this rotation value is used to cyclically rotate the static S-box in each round (i.e. Key dependent S-box rotations). So, 10 rounds of encryption require 150 XOR (150O) operations and 10 round key dependent S-box rotations.

Operation complexity of each block of plain text encryption using dynamic AES with ECB mode, CBC mode and BKG is calculated with further addition of operational complexity of key dependent S-box generation.

Table 4. Operational Complexities with key dependent S-boxes

Algorithm	Operational Complexity Parameters				
	O	M	L	N	H
AES with ECB Mode and Key Dependent S-box	704 + 10 Round key dependent S-box rotations	144	200	0	0
AES with CBC Mode and Key Dependent S-box	720 + 10 Round key dependent S-box rotations	144	200	0	0
AES with BKG and Key Dependent S-box	**748 + 10 Round key dependent S-box rotations**	**144**	**200**	**8**	**1**

The operational complexity of primitive AES when used in conjunction with Block key generation algorithm is slightly high in comparison to primitive AES when used in association with ECB or CBC Mode. In spite of that, parallel implementation of the proposed algorithm significantly reduces the execution time while performing encryption and decryption.

6.2 Avalanche Effect Test

Testing is performed on a set containing two plain texts differ by 1 bit and by keeping the secret key constant. Total 8 sets of plain text samples have been used for the purpose of calculating avalanche effect ranging from 250 to 2000 as shown in Tables 5 to 12.

Table 5. AES using ECB mode and AES using BKG algorithm

Total samples	Number of times both algorithms have given same Avalanche effect	Number of times AES using ECB mode has given better Avalanche effect	Number of times AES using BKG algorithm has given better Avalanche effect
250	14	102	**134**
500	31	224	**245**
750	48	340	**362**
1000	70	441	**489**
1250	81	541	**628**
1500	91	652	**757**
1750	150	766	**880**
2000	119	876	**1005**

Table 6. AES using ECB mode and AES using BKG algorithm with dynamic S-boxes

Total samples	Number of times both algorithms have given same Avalanche effect	Number of times AES using ECB mode has given better Avalanche effect	Number of times BKG algorithm with dynamic S-boxes has given better Avalanche effect
250	18	107	**125**
500	35	226	**239**
750	49	339	**362**
1000	60	439	**501**
1250	69	554	**627**
1500	77	678	**745**
1750	85	794	**871**
2000	97	913	**990**

Table 7. AES using ECB mode with dynamic S-boxes and AES using BKG algorithm

Total samples	Number of times both algorithms have given same Avalanche effect	Number of times ECB mode with Dynamic S-boxes has given better Avalanche effect	Number of times BKG algorithm has given better Avalanche effect
250	7	112	**131**
500	19	218	**263**
750	38	342	**374**
1000	46	443	**511**
1250	28	554	**638**
1500	64	676	**760**
1750	72	791	**887**
2000	87	900	**1013**

Table 8. AES using ECB mode with dynamic S-boxes and AES using BKG algorithm with dynamic S-boxes

Total samples	Number of times both algorithms have given same Avalanche effect	Number of times ECB mode with dynamic S-boxes has given better Avalanche effect	Number of times BKG algorithm with dynamic S-boxes has given better Avalanche effect
250	14	110	**126**
500	27	218	**255**
750	38	338	**374**
1000	45	445	**510**
1250	58	562	**630**
1500	73	685	**742**
1750	84	808	**858**
2000	96	934	**970**

Table 9. AES using CBC mode and AES using BKG algorithm

Total samples	Number of times both algorithms have given same Avalanche effect	Number of times CBC mode has given better Avalanche effect	Number of times BKG algorithm has given better Avalanche effect
250	14	106	**130**
500	30	224	**246**
750	45	346	**359**
1000	62	453	**485**
1250	71	568	**611**
1500	82	693	**725**
1750	97	809	**844**
2000	115	920	**965**

Table 10. AES using CBC mode and AES using BKG algorithm with Dynamic S-boxes

Total samples	Number of times both algorithms have given same Avalanche effect	Number of times CBC mode has given better Avalanche effect	Number of times BKG algorithm with dynamic S-boxes has given better Avalanche effect
250	10	113	**127**
500	18	227	**255**
750	25	348	**378**
1000	42	458	**500**
1250	53	578	**619**
1500	61	710	**729**
1750	72	830	**846**
2000	83	949	**968**

Table 11. AES using CBC mode with dynamic S-boxes and AES using BKG algorithm

Total samples	Number of times both algorithms have given same Avalanche effect	Number of times CBC mode with dynamic S-boxes has given better Avalanche effect	Number of times BKG algorithm has given better Avalanche effect
250	9	108	**133**
500	24	215	**261**
750	33	342	**375**
1000	49	449	**505**
1250	62	561	**627**
1500	79	677	**744**
1750	93	772	**885**
2000	103	895	**1002**

Table 12. AES using CBC mode with dynamic S-boxes and AES using BKG algorithm with dynamic S-boxes

Total samples	Number of times both algorithms have given same Avalanche effect	Number of times CBC mode with dynamic S-boxes has given better Avalanche effect	Number of times BKG algorithm with dynamic S-boxes has given better Avalanche effect
250	13	106	**131**
500	26	221	**253**
750	36	340	**374**
1000	46	460	**494**
1250	56	590	**604**
1500	70	713	**717**
1750	80	827	**841**
2000	90	950	**960**

Avalanche effect comparisons successfully render that proposed algorithm is capable of generating high avalanche effect on random samples in more instances as compared to original AES when used with ECB and CBC mode.

7 CONCLUSIONS

This papers presents an improvement in AES along with modes of operation in consideration. Experimental results clearly manifest that inclusion of Block key generation algorithm enhances the avalanche effect on randomly generated plain text samples. Further, it has been successfully justified that proposed algorithm eradicates the disadvantages of both ECB and CBC modes. However, some enhancements could be introduced in the Block key generation algorithm to reduce its time complexity and with some petty modifications in *Trimmed Output Creator*, proposed algorithm can also be used in AES-192 and AES-256 bit variants. Furthermore, the addition of dynamic S-boxes eliminates any possibility of cryptanalysis and make this algorithm highly useful in security critical systems. Apart from that, proposed algorithm can also be used in synchrony with any of the modern block ciphers.

8 REFERENCES

[1] Daemen, J. and Rijmen, V.: The Design of Rijndael: AES –The Advanced Encryption Standard, Springer-Verlag, 2002.

[2] Daemen, J. and Rijmen, V.: The Block cipher Rijndael, Third International Conference on smart card Research and Applications, Lecture Notes in computer science, Vol.1820, Springer-Verlag, pp. 227-284, 2000.

[3] Federal Information Processing Standards Publications (FIPS 197), Advanced Encryption Standard (AES), 2001.

[4] Federal Information Processing Standards Publications (FIPS 180 - 4), Secured Hash Standard (SHA), 2012.

[5] Jacob, G., Murugan, A. and Viola, I.: Towards the Generation of a Dynamic Key-Dependent S-Box to Enhance Security, International Association of Cryptologic Research, Cryptology ePrint Archive: Report No. 92, 2015.

[6] Krishnamurthy, G. N. and Ramaswami, V.: Making AES Stronger: AES wich Key - Dependent S-Box, International Journal of Computer Science and Network Security, Vol.8, No.9, pp. 388-398, 2008.

[7] Nadaf, R. and Desai, V.: Hardware Implementation of Modified AES with Key Dependent Dynamic S-Box, International Conference on Advanced Research in Engineering and Technology, pp. 576-580, 2013.

[8] Nejad, F. H., Sabah, S. and Jam, A. J.: Analysis of Avalanche Effect on Advanced Encryption Standard by using Dynamic S–Box Depends on Round Keys, International Conference on Computational Science and Technology, pp. 1-5, 2014.

[9] Kazlauskas, K. and Kazlauskas, J.: Key - Dependent S-Box Generation in AES Block Cipher System, INFORMATICA, Vol. 20, No. 1, pp. 23-34, 2009.

[10] Gupta, K. C. and Sarkar, P.: Improved Construction of Non-linear Resiliant S-Boxes, IEEE Transaction on Information Theory, Vol. 51, No. 1, pp. 341-358, 2005.

[11] Juremi, J., Mahmod, R., Sulaiman, S. and Ramli, J.: Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key, International Journal of Cyber-Security and Digital Forensics, Vol. 1, No. 3, pp. 183-188, 2012.

[12] Fahmy, A., Shaarawy, M., El-Hadad, K., Salama, G. and Hassanain, K.: A Proposal for a Key-Dependent AES, 3rd International Conference on Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia, 2005.

[13] Ferguson, N., Schroeppel, R. and Whiting, D.: A Simple Algebric Representation of Rjindael, Selected Areas in Cryptography, Lecture Notes in Computer Science, Vol. 2259, pp. 103-111, 2001.

[14] Kazlauskas, K., Vaicekauskas, G. and Smaliukas, R.: An Algorithm for Key-Dependent S-Box Generation in Block Cipher System, INFORMATICA, Vol. 26, No. 1, pp. 51-65, 2015.

[15] Abhiram, L. S., Gowrav, L., Kumar, P. H. L., Sriroop, B. K. and Lakkanavar, M. C.: Design and Synthesis of Dual Key based AES Encryption, International Conference on Circuits, Communication, Control and Computing, pp. 85-88, 2014.

[16] Stoinov, N.: One Approach of using Key-Dependent S-BOXes in AES, Multimedia communications, Services and Security, Communications in computer and information science, Vol. 149, pp. 317-323, 2011.

[17] Juremi, J., Mahmod, R. and Sulaiman, S.,: A proposal for improving AES S-box with Rotation and Key-Dependent, International Conference on Cyber Security, Cyber Warfare and Digital Forensic, pp. 38-42, 2012.

[18] Wenceslao, F. V. Jr.: "Performance Efficency of Modified AES Algorithm using Multiple S – Boxes", International Journal of New Computer Architectures and their Applications, Vol. 5, No. 1, pp. 1-9, 2015.

[19] Sahoo, O. B., Kole, D. K. and Rahman, H.: An Optimized S-Box for Advanced Encryption Standard (AES) Design, International Conference on Advances in Computing and Communications, pp. 154-157, 2012.

[20] Isa, H., Bahari, I., Sufian, H. and F Z'aba, M. R.: AES: Current Security and Efficency Analysis of its Alternatives, 7th International Conference on Information Asurance and Security, pp. 267-274, 2011.

[21] Gong, J., Liu, W. and Zhang, H.: Multiple Lookup Table-Based AES Encryption Algorithm Implementation, International Conference on Solid State Devices and Materials Science, pp. 842-847, 2012.

[22] Pradeep, L. N. and Bhattacharjya, A.: Random Key and Key Dependent S-box Generation for AES Cipher to Overcome Known Attacks, Security in Computing and Communication, Communications in Computer and Information Science, Springer-Verlag Vol. 377, pp. 63-69, 2013.

[23] Najaftorkaman, M. and Kazazi, N. S.: A Method to Encrypt Information with DNA-Based Cryptography, International Journal of Cyber-Security and Digital Forensics, Vol. 4, No. 3, 2015.

[24] NIST Computer Security Division's (CSD) Security Technology Group (STG), Block Cipher Modes, Cryptographic Toolkit, 2014.

[25] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation, 2011.

[26] Webster, A. F. and Tavares, S. E.: On the Design of S-Boxes, Advances in Cryptology, Crypto'85, Lecture Notes in Computer Science, Springer-Verlag, Vol. 218, pp. 523-534, 1986.

[27] Ferguson, N., Schneier, B. and Kohno, T.: Cryptography Engineering: Design Principles and Practical Applications, Wiley Publishing, 1st Edition, 2010.

[28] Paar, C. and Pelzl, J.: Understanding Cryptography, Springer Publishing, 1st edition, 2012.

[29] Stallings, W.: Cryptography and Network Security, Pearson Education, 6th edition, 2013.

[30] Frouzan, B. A. and Mukopadhyay, D.: Cryptography and Network Security, Mcgraw Hill Education, 2nd edition, 2011.

[31] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

[32] https://en.wikipedia.org/wiki/Rijndael_S-box

[33] https://www.random.org/bytes/

[34] https://en.wikipedia.org/wiki/Random_number_generation

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(1): 46-60
The Society of Digital Information and Wireless Communications, 2016 (ISSN: 2305-0012)

Text-Based Age and Gender Prediction for Online Safety Monitoring

Janneke van de Loo and Guy De Pauw and Walter Daelemans
CLiPS - Computational Linguistics Group – University of Antwerp
Prinsstraat 13, 2000 Antwerpen, Belgium
firstname.lastname@uantwerpen.be

ABSTRACT

This paper explores the capabilities of text-based age and gender prediction geared towards the application of detecting harmful content and conduct on social media. More specifically, we focus on the use case of detecting sexual predators who try to "groom" children online and possibly provide false age and gender information in their user profiles. We perform age and gender classification experiments on a dataset of nearly 380,000 Dutch chat posts from a social network. We evaluate and compare binary age classifiers trained to separate younger and older authors according to different age boundaries and find that macro-averaged F-scores increase when the age boundary is raised. Furthermore, we show that use-case applicable performance levels can be achieved for the classification of minors versus adults, thereby providing a useful component in a cybersecurity monitoring tool for social network moderators.

KEYWORDS

author profiling, cybersecurity, social media, online safety, grooming

1 INTRODUCTION

The advantages, fun, and opportunities social media bring for children are offset by significant potential dangers. According to a pan-European survey[1], children spend a lot of time on social media interaction without parental supervision (in their bedroom or as mobile users) and are relatively often exposed to dangerous situations. Twelve percent of 9 to 16 year old youngsters report having been bothered or upset during social media use, mainly by exposure to bullying or unwanted sexual content. Although much less frequent, they all too often report attempts at grooming by adults. In this paper we show how author profiling, a text mining area, can be applied to the detection of harmful content in social media, and illustrate this by means of age and gender profiling for the detection of grooming by pedophiles in social media.

The last decade has seen a large improvement in the accuracy and applicability of techniques for knowledge discovery from text (also called *text mining* or *text analytics*). The type of knowledge extracted can be factual, for example for use in medical expert systems (IBM's Watson for oncology application is a good example [1]), or it can be subjective as in the many sentiment analysis applications where opinions or sentiments of authors are targeted (see [2,3] for applications to political media coverage analysis and economic prediction).

In this paper, we look at a more recent type of knowledge discovery from text, namely author profiling: the extraction of demographic and psychological characteristics of authors from text they have written [4,5]. This is often called *computational stylometry* [6]. By analyzing the linguistic properties of text, "metadata" such as age, gender, region, and personality traits of the author can be estimated on the basis of machine learned models trained on text samples written by authors for which the profile is known. Author profiling has established itself as a text analytics subarea with its own conferences and shared task competitions, for instance the shared tasks at the PAN workshops [7,8,9,10]. Many applications of author profiling have been proposed, ranging from demographic marketing to forensic detection tasks such as those described in this paper.

In the **AMiCA**-project[2], author profiling is used as one of the modules in a system for detecting three

[1] Available from http://www.eukidsonline.net

[2] http://www.amicaproject.be

harmful situations for children in social networks: depression and suicide announcements [10], cyberbullying [12], and sexually transgressive behavior (including grooming by pedophiles [13]). All three of these applications involve content-based text analysis. For example, to detect suicidal children, negative emotions or suicide announcements should be recognized in text, and cyberbullying mostly involves the expression of threats, defamation or insults. But in addition to this factual knowledge extraction, profile information can help as well. Especially age, gender, and personality information can improve the detection of these harmful events when combined with the factual knowledge. For example, there are clear correlations between gender and personality on the one hand, and the probability of being a victim or bully in cyberbullying events, and there are links between personality and risk of depression and suicidal behavior.

This paper is concerned with the application of author profiling information (in this case the detection of age and gender) in the **AMiCA** use case concerned with identifying grooming by pedophiles in social networks. It combines a module detecting sexual content and the specific vocabulary of grooming with a module comparing the profile provided by the user to the profile that is induced from the text produced by this user. The architecture is as follows: when there is a mismatch between the induced and the provided profile (for example a provided profile of a 14-year-old girl does not match with the induced profile of an adult male), the content of the interaction is analyzed by a classifier detecting sexual content and grooming behavior, and if that classifier also returns a positive result, the interaction is reported to the moderator of the social network.

In this monitoring support set-up, it is important that the text analysis classifiers return high recall rather than high precision: it is better to err on the side of false positives than on the side of false negatives, as there will be manual inspection by the moderator anyway before taking action. Sufficiently high recall ensures that no harmful cases are missed, while even modest precision dramatically reduces the number of interactions that need to be manually monitored.

A crucial component in this profiling application is the set-up of the age and gender detection task. The success of age classification partly depends on the age classes that are being distinguished. In our current set-up, we carry out binary age prediction, i.e. determining whether authors are older or younger than a specific age boundary. Working with only two classes (minors versus adults) not only ties in with the intended application, but also serves to maximize classification accuracy. Furthermore, the age boundary itself can be easily adapted to any number that is relevant to the specific use case at hand, based on legal constraints (e.g. the legal age of sexual consent) or age related statistics (e.g. sexual offense rates across age groups). The goal of this paper is to show that the profiling module can be optimized to achieve accuracy levels that are useful for our decision support system for social network moderators.

We will start with a brief overview of related age and gender prediction research (Section 2), followed by a description of the dataset and the methods employed in our current research (Section 3). In Section 4, we present the results of our age and gender classification experiments and discuss the implications of these results for the use case of sexual predator detection. We finish with concluding remarks and outline our plans for future research in Section 5.

2 RELATED RESEARCH

Early work in automatic author profiling was done by [4], who categorized formal written texts from the British National Corpus by author gender. A few years later, age and gender prediction studies became increasingly focused on informal online social media texts, especially on blogs (e.g. [14,15,16,17] and tweets [18,19,20,21], but also on chat posts [13] and YouTube comments [22]. This trend is also reflected in the author profiling tasks that were organized at PAN 2013, 2014 and 2015 [8,9,10].

Various supervised machine learning algorithms have been employed, using a variety of textual features, such as character n-grams, token n-grams, part-of-speech n-grams, specific token subsets (e.g. emoticons, internet acronyms, function

Table 1. The list of classification experiments and the associated classes.

Task	Classes
Age	YOUNGER < age_boundary ≤ OLDER
Gender	♀ - ♂
Age & Gender	YOUNGER♀ - OLDER♂ - YOUNGER♂ - OLDER♀

words, LIWC[3] dictionaries), readability features (e.g. average word and sentence length), character-based stylistic features (e.g. capitalization, character repetitions, punctuation), and extracted topics. In some cases, extratextual profile features were used as well, for instance the number of friends and followers [22,18,24], background colors [25], and posted images [25]. Our current study is limited to features extracted from the written texts.

Binary age prediction, as researched in this paper, was first performed by [22], who predicted whether bloggers were under or over 18. They experimented with shallow textual features based on character counts, language models, and meta-information such as the number of friends. The resulting performance was not far above the majority baseline, however. [27] carried out binary age prediction experiments on transcribed telephone conversations and [18] on tweets. They used the age boundaries 40 and 30, respectively, to separate the two age classes, and in both studies the features used for classification were token n-grams and sociolinguistic features. [13] used token and character n-grams to predict whether authors of Flemish Dutch chat posts from the social network Netlog, were under or over 16. In addition, they studied the effect of increasing the gap between the older and the younger age group. This paper presents experiments on expanded data sets from the same social network. [28] studied the task of predicting whether blog authors were born before or after a specific year. Like in the present study, they experimented with different class boundaries, but they used birth year rather than age to define those boundaries, as their aim was to find a boundary between two generations. This is an important difference, since the blog data per author included posts written at different ages, over periods of up to ten years. In contrast, our research aims at an application that distinctly requires an age-oriented approach, due to the legal context of the application.

[3] http://www.liwc.net

3 MATERIAL AND METHODS

In order to detect illegal grooming activity involving minors, we need reliable age and gender assignment to determine the ages of the participants in the conversation, or to detect mismatches between the (possibly false) profile provided by a user and the demographic data as inferred from the text.

3.1 Experimental Setup

We conduct age and gender prediction experiments on a dataset of social network posts, which is described in subsection 3.2. Three types of prediction experiments are carried out: age prediction, gender prediction and combined age and gender prediction. Age prediction is defined as a binary classification task, i.e. predicting whether an author is older or younger than a certain age boundary. We vary this boundary between 16 and 28. The experiment types and the associated classes are listed in Table 1.

For each experiment type, we carry out five-fold cross-validation experiments (i.e. using 80% of the data for training and 20% for testing in each fold), both on the full, unbalanced, dataset and on data subsets balanced for age class and gender. The experiments on the full dataset showcase the performance on real-life data, while the experiments on the balanced data subsets allow us to perform a more detailed analysis of the observed effects, by factoring out effects of class imbalance.

3.2 Dataset

The full dataset consists of 379,769 chat posts from the Belgian social networking website Netlog[4]. The posts are interpersonal chat messages which were posted in the public social networking environment (as opposed to private messages, which could not be made available by Netlog).

[4] Netlog ceased activitities in 2014 and has since been merged with Twoo.

(a)

(b)

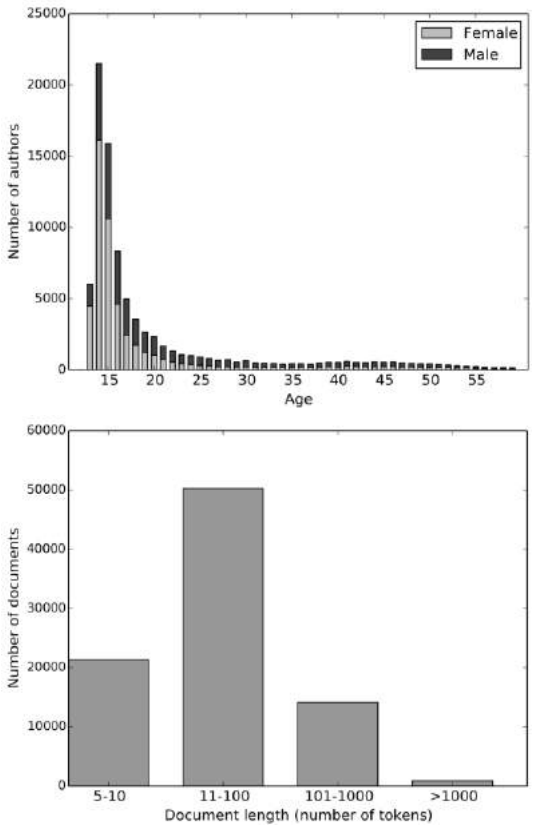


Figure 1. Distribution information for the full dataset.

They were posted between November 2010 and February 2011 by 86,610 different users. For each user, the self-reported age, gender and location was available in the Netlog user profile. Only Dutch posts (classified as such by a language identification system[5]) from Belgian users were included, with a minimum post length of 5 tokens. The dataset contains a large amount of non-standard language, typical of user-generated content. The non-standard forms include spelling errors, unofficial abbreviations (some of which are common in internet language) and various creative spelling variants, which often adopt characteristics from colloquial speech, including regional dialect influences [29].

The ages of the users range from 11 to 59. Figure 1(a) shows the age and gender distribution of the users in the dataset. There is a very high peak at the ages of 14 and 15, with over 20,000 and over 15,000 users respectively, whereas for the 25+ ages, the dataset contains fewer than 1,000 users per age category. For the ages 11 and 12, the number of authors is below 10. In the ages 13 to 15, females are markedly overrepresented, with percentages between 69% and 75%, whereas between the ages 23 and 32, males are slightly overrepresented: between 60% and 67% of the users in those age categories are male.

For our profiling experiments, we concatenated all posts per user into one document, thus yielding 86,610 single-user documents for training and testing. The distribution of document lengths is shown in Figure 1(b). The group of documents with 11 to 100 tokens is largest (about 50,000 documents) and only a small number of documents consist of more than 1,000 tokens.

3.2 Balanced Data Subset

For the prediction of age classes (older or younger with respect to a specific age boundary) and the prediction of combined age and gender classes, we constructed data subsets that are balanced for age class and gender; one for each age boundary. So for instance, for the prediction of the age class with respect to the age boundary of 16 (-16 or 16+), we constructed a data subset with equal amounts of -16 female authors, -16 male authors, 16+ female authors, and 16+ male authors in each of the five partitions. For each age boundary, the number of randomly selected documents per class per partition was the same: 1,165 documents.

This resulted in partitions of 4,660 documents each, so 23,300 documents in total per balanced data subset. The resulting age and gender distributions in four of the balanced subsets (viz. the subsets for age boundaries 16, 18, 22 and 28, respectively) are shown in Figure 2. Due to the random selection of documents per class, the original age distribution within each class is preserved.

For the prediction of gender only, a data subset balanced only for gender was constructed. This data subset consists of 7,006 documents per gender per partition, so 14,012 per partition and 70,060 in total.

3.2 Classifier and Features

The classifier we used is a Support Vector Machine (SVM) classifier with a linear kernel, viz.

[5] Available from http://textgain.com

(a)

(b)

(c)

(d)

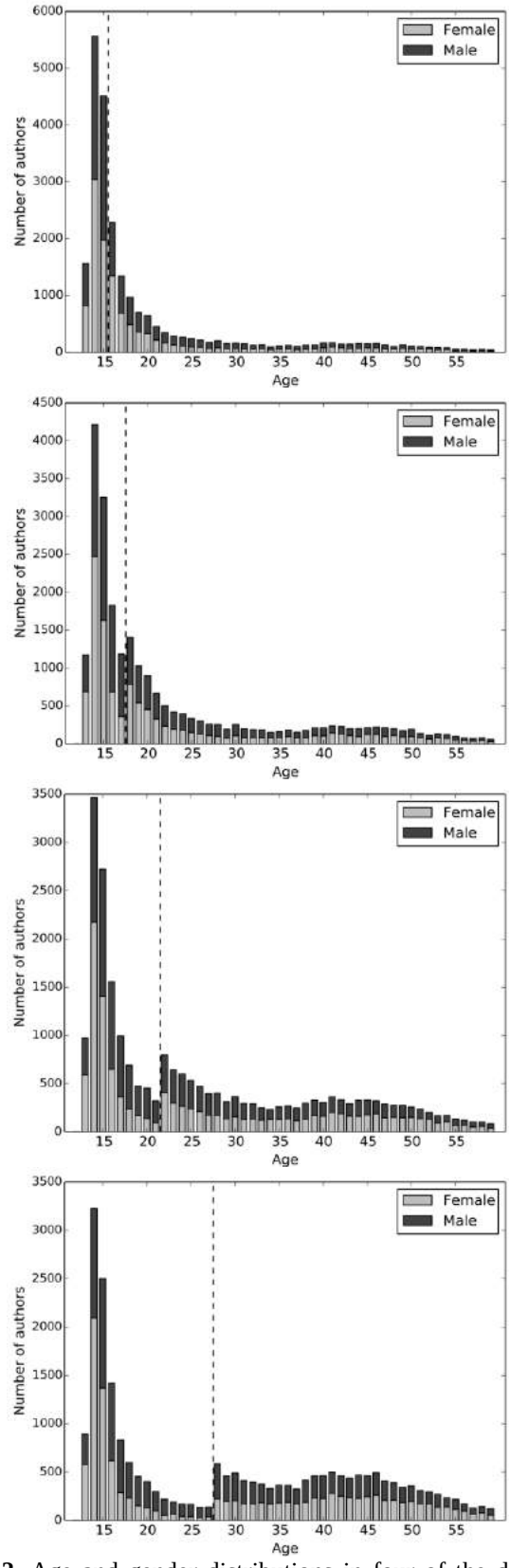


Figure 2. Age and gender distributions in four of the data subsets balanced for age class and gender, viz. the subsets balanced according to age boundaries 16 (a), 18 (b), 22 (c), and 28 (d). In each graph, the age boundary is marked with a vertical dashed line.

scikit-learn's LinearSVC classifier [30]. For each fold, the classifier's parameter *C* was tuned in a 3-fold cross-validation grid search on the training set.

The features used for classification are token and character n-grams. Token n-grams have been widely used for age and gender prediction and have shown good results [14,18,13,20]. Before tokenization, we carried out a number of text preprocessing steps. All uppercase alphabetic characters were converted to lowercase and character repetitions were reduced to a maximum of 3 (e.g. 'hiiiii' → 'hiii'), to obtain a certain level of generalization across different varieties of the same word. For generalization purposes, emoticons, URLs, e-mail addresses, and links to photos and videos were replaced by a single special character.

The character n-grams, on the other hand, were collected from the original, raw text, i.e. without carrying out the preprocessing steps discussed above. The character n-grams can capture many stylistic characteristics, such as (parts of) emoticons, character repetitions, capitalization and morphological features. In addition, the fact that they capture parts of words renders them more robust to spelling variants and errors, which are numerous in these chat data. Furthermore, they capture stylistic tendencies that authors are often less aware of, making it harder for sexual predators to deceive the system. Some other age and gender prediction studies in which character n-grams have been successfully used, are [13], [31], and [32].

Only the n-grams with the highest relative frequencies in the training set were selected, imposing a threshold on the total number of n-grams of each type to be considered by the classifier. An n-gram's relative frequency is the count of the n-gram normalized by the total number of n-grams (of that type) in the document. We selected a relatively high number of character n-grams compared to the number of token n-grams, as the number of high-frequency character n-grams is relatively large.

The list of features is thus as follows:

- the 2,500 most frequent token unigrams;
- the 2,500 most frequent token bigrams;
- the 5,000 most frequent character trigrams;
- the 5,000 most frequent character tetra-grams.

3.2 Evaluation Measures

For each fold in each five-fold cross-validation experiment, several evaluation scores were calculated, based on the system's age and gender predictions for the test documents. The calculated scores are precision, recall and F_1-score per class and the overall accuracy and macro-averaged F_1-score. Scores were averaged across the five folds. Accuracy scores were compared to baseline accuracy scores produced by a system that always predicts the majority class.

The age and gender information provided in the users' Netlog profiles was used as gold standard class information. Although this profile information is not fully reliable, we assume that the portion of obfuscated profile information in our data is sufficiently small to appropriately train and evaluate the classifier.

4 RESULTS AND DISCUSSION

In this section, we discuss the results for the three prediction tasks: age prediction, gender prediction and combined age and gender prediction. For each task, we perform five-fold cross-validation experiments, and compare the results produced with the full, unbalanced, dataset to the results produced with balanced subsets. The reported scores are the average scores across five folds. In the graphs that include error bars, these error bars indicate the 95% confidence intervals, based on the standard deviations of the scores across the five folds.

4.2 Age Prediction

Figure 3(a) displays the age prediction scores for the different age boundaries on the full, unbalanced dataset. The accuracy rises from 76.7% with age boundary 16 to 91.7% with age boundary 28. The curve is quite steep in the beginning and starts to level off towards the end. The macro-averaged F-score reaches a maximum of 84.8% at age boundary 23 and slowly decreases after that.

As we see in Figure 3(b), the rise in the accuracy score is mainly due to increased precision and recall scores for the younger class. This is caused partially by the growing class imbalance: as the

(a)

(b)

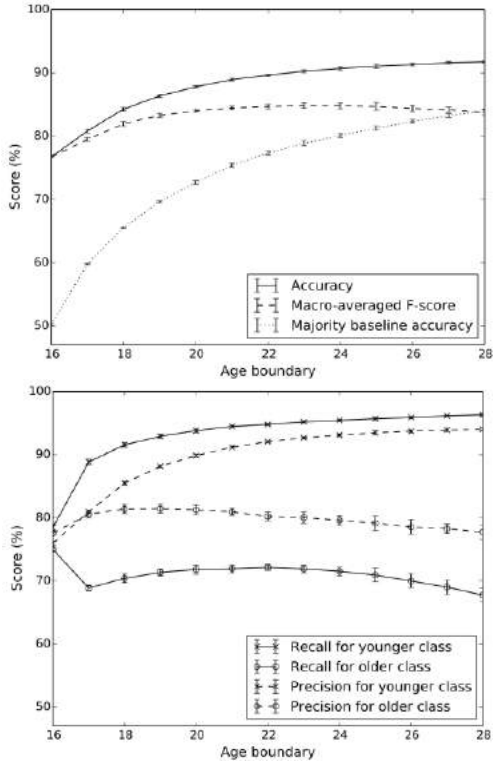


Figure 3. Age prediction scores (overall (a) and per class (b)) with the unbalanced dataset.

age boundary rises, the portion of instances in the younger class grows, which has a positive effect on the scores for this class. The growing class imbalance is also reflected in the rise of the majority baseline in Figure 3(a). Still, the accuracy curve in Figure 3(a) remains far above the baseline. The precision and recall scores for the older class remain reasonably stable and show a moderate decrease at the end, which causes the slight decline in the macro-averaged F-score after age boundary 23.

Figure 4 shows the results when the effect of increasing class imbalance is eliminated. In Figure 4(b), we can see that with data subsets balanced for age class (and gender), the precision and recall scores for both classes rise. Consequently, the macro-averaged F-score also keeps rising.

In addition to the scores per age class, it is also important to know how the age classifiers perform for authors of specific ages. Figure 5 shows the age prediction accuracies per age for four different age boundaries, produced with the unbalanced dataset. Figure 6 shows the same for four balanced data subsets; they are the same subsets for which the age distributions are depicted in Figure 2. All

(a)

(b)

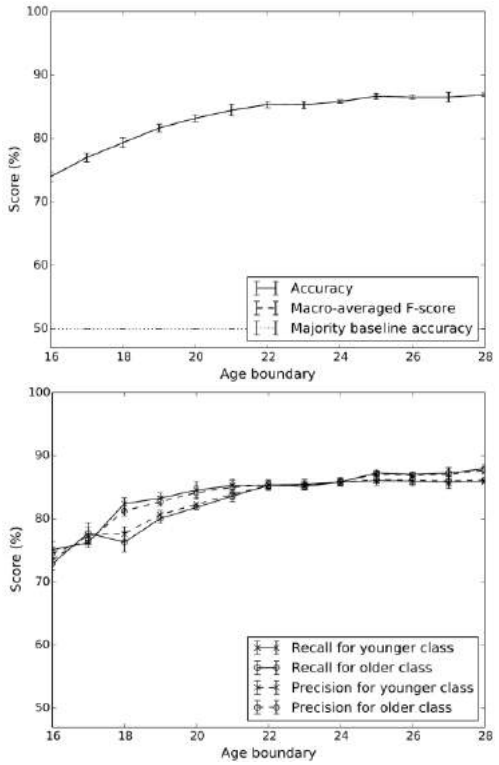


Figure 4. Age prediction scores with the balanced data subsets. In (a), the macro-averaged F-scores are not visible, as they almost fully overlap with the accuracy scores. The majority baseline accuracy in (a) is at a constant level of 50%, regardless of the age boundary.

graphs in Figure 5 and Figure 6 show a clear accuracy drop around the chosen age boundary. This means that texts by authors with ages close to an age boundary are harder to classify, because they are relatively similar to texts by authors close to the other side of the boundary.

With the unbalanced dataset (Figure 5), the minimum of the drop is always at the age just above the age boundary and the drop is much steeper on the left side than on the right side. As the age boundary rises, the drop gets wider, especially on the right side, which means that the scores for the higher ages decrease. The shape of the drop is partly related to the age distribution in the dataset, as can be seen when comparing the graphs for the unbalanced dataset (Figure 5) with those for the balanced data subsets (Figure 6) and by relating them to the age distributions in Figure 1(a) and Figure 2.

(a)

(b)

(c)

(d)

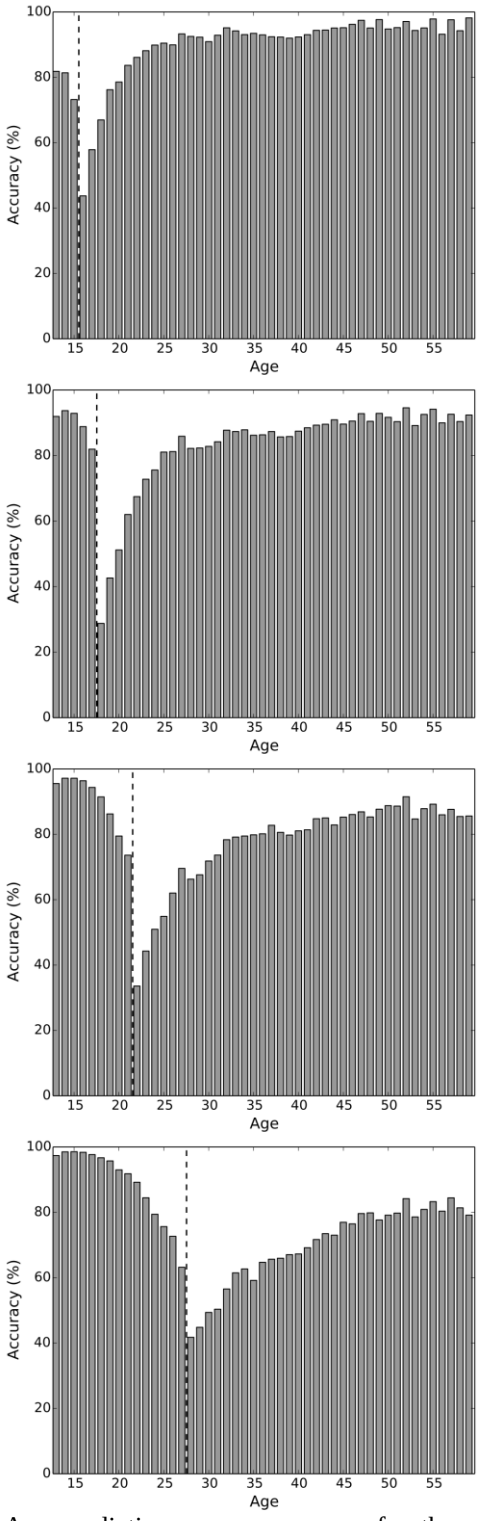


Figure 5. Age prediction: accuracy scores for the unbalanced dataset, when predicting age with respect to four different age boundaries: 16 (a), 18 (b), 22 (c), and 28 (d). In each graph, the ages on the x-axis are the true ages of the authors, the scores on the y-axis are the age prediction accuracies produced for the authors of that specific age, and the vertical dashed line marks the age boundary.

(a)

(b)

(c)

(d)

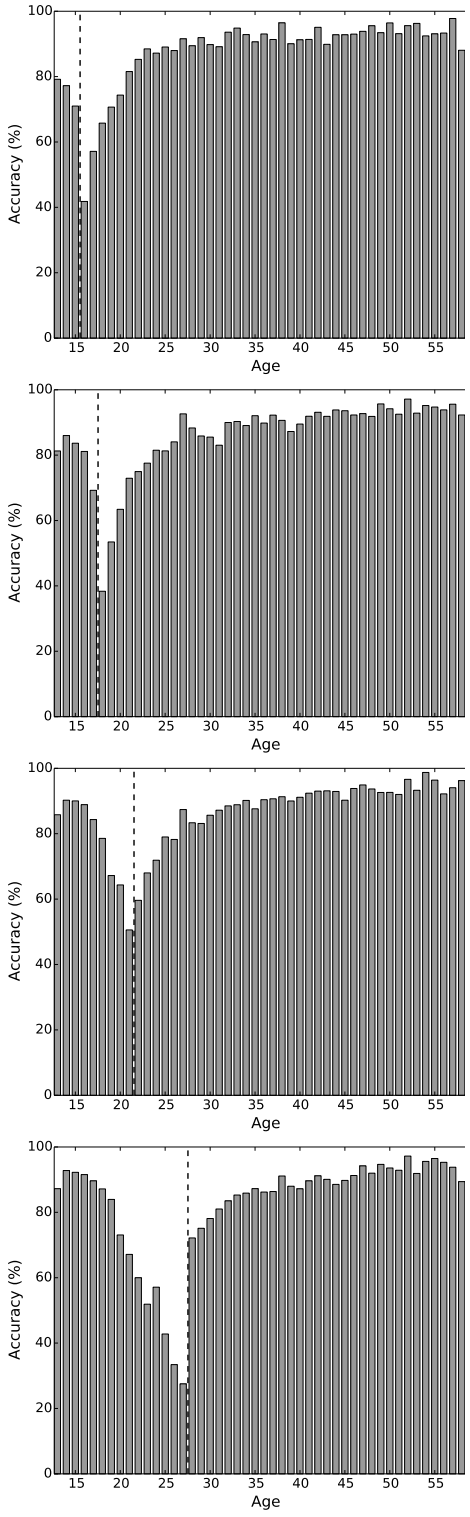


Figure 6. Age prediction: accuracy scores per age with the balanced data subsets, when predicting age with respect to four different age boundaries: 16 (a), 18 (b), 22 (c), and 28 (d). In each graph, the ages on the x-axis are the true ages of the authors, the scores on the y-axis are the age prediction accuracies produced for the authors of that specific age, and the vertical dashed line marks the age boundary.

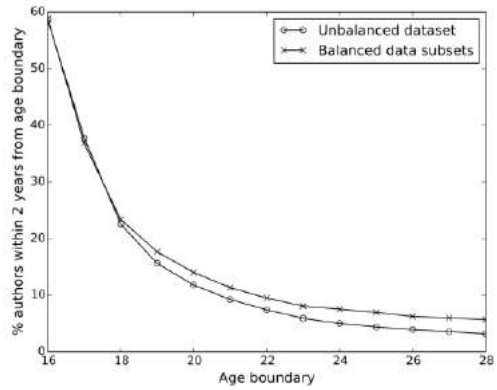


Figure 7. Percentage of authors within 2 years from the age boundary in the unbalanced dataset and in the balanced data subsets.

The effect of closeness to age boundary also plays a role in the increase of the accuracy scores in Figure 3 and Figure 4. As the age boundary increases, the percentage of authors close to it decreases, since the high peak in the age distribution is situated at the lower ages (cf. Figure 1(a)). This effect is shown in Figure 7; it is not only present in the unbalanced dataset, but also in the balanced data subsets. As a result, the average age prediction accuracy rises when the age boundary increases, since the accuracy scores are relatively high for authors further from the age boundary. However, it is unknown to what extent this factor influenced the scores, and excluding both this factor and the factor of class imbalance at the same time is impossible with this dataset.

As expected, another important factor that affects the age classification performance is the length of the document that is classified: on average, longer documents are classified more accurately than shorter documents. Figure 8 shows the macro-averaged F-scores for different document length categories, produced with the full dataset. For the most frequent document length category in the dataset, with documents of 11 to 100 tokens (see Figure 1(b)), the macro-averaged F-scores range between 77.8% and 85.6%, depending on the age boundary. However, for short documents, with only 5 to 10 tokens, the macro-averaged F-scores are still reasonable: they are between 68.4% and 76.9%. When the documents contain more than 1,000 tokens, scores are above 90% for all age boundaries except age boundary 16 (they range between 86.8% and 93.4%).

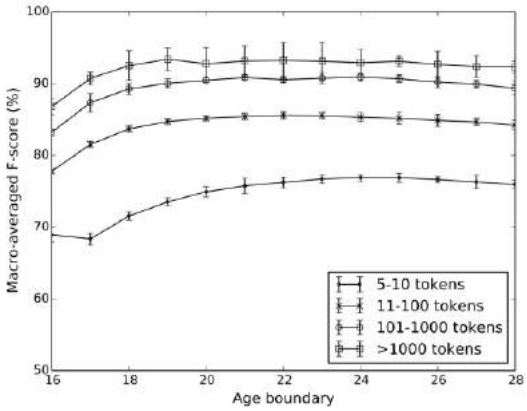


Figure 8. Age prediction scores per document length (i.e. number of tokens in the document) with the unbalanced dataset.

4.2 Gender Prediction

The gender prediction scores are shown in Table 2. The accuracy with the data subset balanced for gender is very similar to the accuracy with the full dataset, even slightly higher, although the dataset is a bit smaller (70,060 vs. 86,610 documents). With the full dataset, the precision and recall scores for the female class are higher than the scores for the male class, especially the recall scores (79.7% vs. 53.0%). This is probably due to the class imbalance (51,269 female authors vs. 35,341 male authors), as with the balanced data subsets, the recall for the female class is *lower* than the recall for the male class (65.8% vs. 72.7%).

4.3 Combined Age and Gender Prediction

Figure 9 displays the overall scores for the combined age and gender prediction task. These scores were produced by training the system on the four combined classes (cf. Table 1) and then predicting the same four classes in the test set. We also carried out experiments in which we predicted age and gender separately (with two systems, trained on the separate binary classes) and then combined

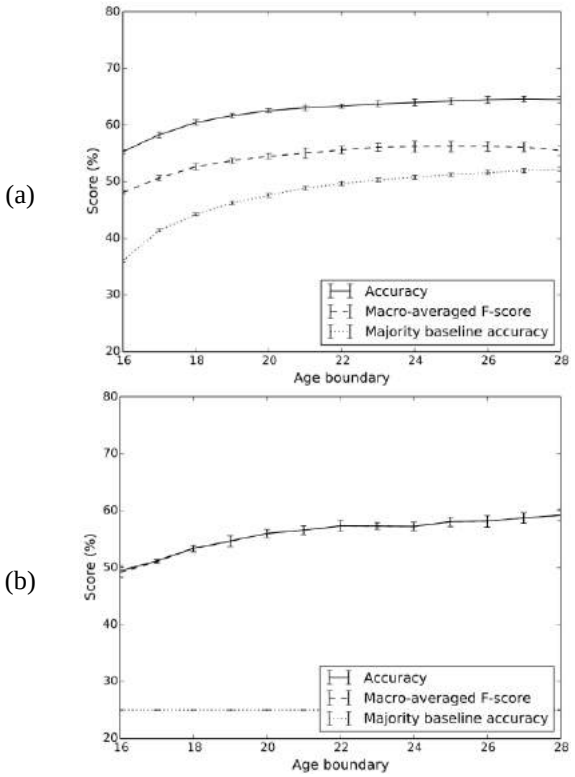


Figure 9. Combined age and gender prediction: overall scores per age boundary, produced with the unbalanced dataset (a) and the balanced data subsets (b). In (b), the macro-averaged F-scores are not visible, as they almost fully overlap with the accuracy scores. The majority baseline accuracy in (b) is at a constant level of 25%, regardless of the age boundary.

the resulting age and gender predictions afterwards. This resulted in very similar scores (not shown here), only with a much larger variance across folds.

In Figure 9(a), which shows the scores with the unbalanced dataset, we see the accuracy score increase again as the age boundary rises, as in Figure 3(a), but the curve starts to level off earlier and the differences are smaller. The accuracy scores range between 55.3% (at age boundary 16) and 64.6% (at age boundary 27) and exceed the majority baseline accuracies by 12.3% to 19.2%. The macro-averaged F-score reaches its maximum of 56.2% at age boundary 26 and then slowly starts

Table 2. Gender prediction scores on the full dataset and on the data subset balanced for gender, averaged across five folds. Macro F = macro-averaged F-score.

	Overall Scores		Scores for ♀			Scores for ♂		
Dataset	**Accuracy**	**Macro-F**	**Precision**	**Recall**	**F-score**	**Precision**	**Recall**	**F-score**
Full	68.8	66.6	71.1	79.7	75.1	64.2	53.0	58.0
Balanced	69.3	69.2	70.7	65.8	68.2	68.0	72.7	70.3

degrading again. With the balanced subsets (cf. Figure 9(b)), the accuracy rises from 49.5% to 59.2%, as does the macro-averaged F-score.

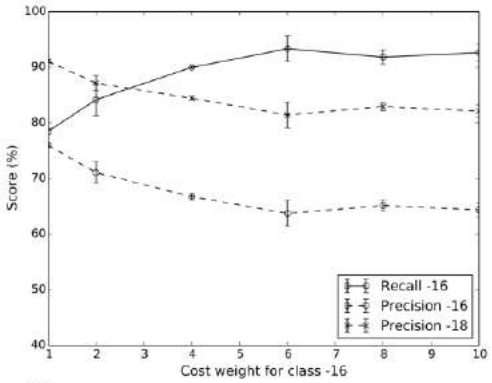
4.3 Consequences for the Application

For the application of sexual predator detection, one of the most important aims is to distinguish authors above and below the age of consent for sexual activity, which is currently age 16 in Belgium. We need a -16 classifier to detect the potential victims and a 16+ classifier to detect the potential offenders. For both classifiers, a high recall is most important, but the precision should also be reasonably high to minimize the number of manual interventions by moderators. In addition, accurate classification of -16 and 18+ authors has the highest priority.

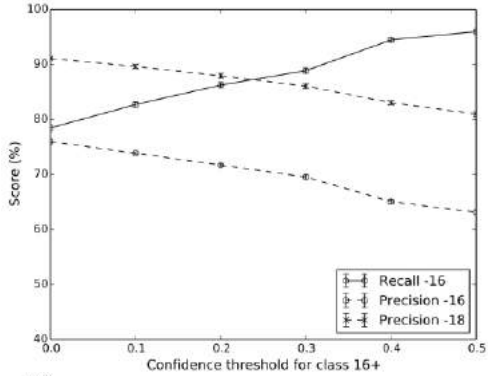
With our current unbalanced dataset, the recall of the -16 classifier (with -16 as the positive class) is 78.5% and its precision is 76.0% (cf. the scores for the younger class in Figure 3(b) at age boundary 16). As we can see in Figure 5(a), a large part of the errors pertain to authors that are just above the boundary. Since our focus is mainly on the correct classification of -16 and 18+ authors, we also calculated a more lenient precision score, which excludes the 16-year-olds and 17-year-olds from the false positives. This score, which we call "precision -18", computes the percentage of -18 authors within the group of authors classified as -16. For our -16 classifier, the "precision -18" score is 91.1%, i.e. much higher than the standard precision score ("precision -16"). This illustrates that a large portion of the false positive authors are 16 or 17 years old.

The 16+ classifier (with 16+ as the positive class) has a recall of 75.0% and a precision of 77.5% on our dataset (cf. the scores for the older class in Figure 3(b) at age boundary 16). Also for this classifier, we calculated a more lenient score, focusing on the 18+ authors. The recall for 18+ authors ("recall 18+") is 86.6%, which is again much higher than the recall score for 16+ authors. The high recall for 18+ authors is also visible in Figure 5(a); this figure shows the accuracy scores for the specific ages, which correspond to the recall scores per age. As age increases, the recall scores rise, until they start leveling off after age 25 and consistently stay between 90% and 98%.

(a)



(b)



(c)

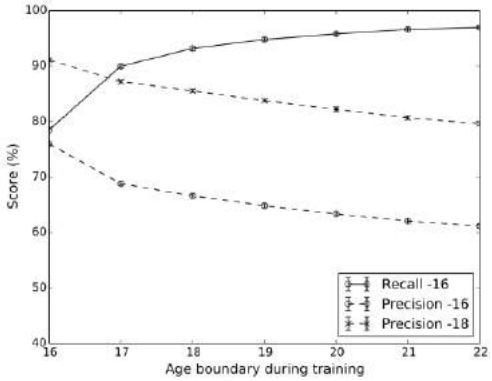


Figure 10. Precision and recall scores for the -16 classifier when using different methods to improve the recall of the class -16: (a) changing cost weight, (b) changing confidence threshold, and (c) changing age boundary during training.

The recall of the -16 classifier, which is important for our application, could be increased in several ways. A standard method for improving recall is to use a higher cost weight for the positive class (-16) during training. Another way is to use the confidence scores that are produced by the SVM classifier (based on an instance's distance to the hyperplane): if an instance is classified as 16+ with a low confidence score, below a specific threshold, classify it as -16 instead of 16+. A third option is to increase the age boundary that is

(a)

(b)

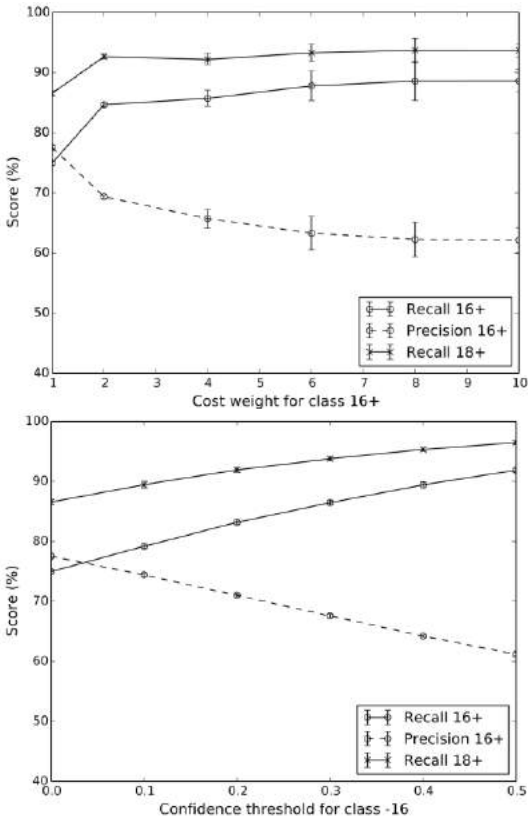


Figure 11. Precision and recall scores for the 16+ classifier when using different methods to improve the recall of the class 16+: (a) changing cost weight, (b) changing confidence threshold.

used for training. As Figure 5 shows, the recall for ages 13 to 15 gets higher when the age boundary rises. So we can train the classifier with instances labeled with the classes "younger" and "older" according to a higher age boundary (e.g. boundary 17), use this classifier to label the test set, and evaluate the resulting labels "younger" and "older" according to the age boundary 16.

We applied the three methods in 5-fold cross-validation experiments on our full, unbalanced dataset, to explore the effects of the different methods on the precision and recall scores. The results are shown in Figure 10. We see that we can achieve recall scores between 90% and 95% with precision scores between 65% and 70%. In addition, the gap between the standard precision score ("precision -16") and the "precision -18" score is very large, especially when we increase the age boundary during training (Figure 10(c)), which means that a large portion of the false positives consists of 16-year-old and 17-year-old authors. With age boundary 17, for instance, recall is 90.0%, with a "precision -16" score of 68.8% and a "precision -18" score of 87.2%.

With cost weight 4 and confidence score 0.3, the recall scores are very similar to the recall with age boundary 17, but the precision scores are less favorable. With cost weight 4, both "precision -16" and "precision -18" are lower (66.7% and 84.4%, respectively). With confidence threshold 0.3, "precision -16" is comparable but the gap between "precision -16" and "precision -18" is a bit smaller (18.4% vs. 16.5%). These tendencies also apply at other comparable recall scores.

Although these exploratory experiments do not show how these results generalize to new data (since we did not use a development set to tune towards high recall in these experiments), the results do show that all three methods are worth considering to improve recall of the -16 class in our final application and that practically usable performance levels can be attained using these methods. Other methods that could be considered are cost-sensitive learning methods such as cost-proportionate rejection sampling [33], in which the negative class is repeatedly downsampled and results are combined in an ensemble set-up.

The methods that use cost weights and confidence thresholds can also be used to improve the recall of the 16+ classifier. The resulting precision and recall scores are shown in Figure 11. The method of moving the age boundary cannot be used here, since we can only increase the age boundary with our current dataset, which decreases the recall for the 16+ class. When we compare the average scores of the two methods for which recall scores for class 16+ are similar, we see that the precision scores and "recall 18+" scores are either very similar or more favorable for the method with the adapted confidence thresholds. Notably, adapting the cost weights yields a much larger score variance across folds and therefore less stable results. With confidence threshold 0.2, recall is 83.2% for 16+ authors and 91.9% for 18+ authors, at a precision of 71.0% for 16+ authors. These are also practically usable scores for detecting potential child groomers.

In addition, gender prediction can be used to detect disagreement between the self-reported gender in a user's profile and the profiling system's

gender prediction for that user. Usually, when a user provides false gender information for child grooming purposes, the user is a man who pretends to be female. Unfortunately, the recall for male authors with our unbalanced dataset was only 53.0% (cf. Table 2). Also here, the recall for the male class could be improved by using techniques such as increasing the cost weight for the male class or increasing the confidence threshold for the female class. When combined with content-based information and age prediction, gender discrepancy can be a useful extra cue for sexual predator detection.

4.4 Additional Features

So far, we have only considered character and token n-grams as relevant features towards classification. In a final set of experiments, we investigated the applicability of additional features, provided by the CLiPS profiling software PROFL[6]. These are part-of-speech n-grams, sentiment features (polarity score), LIWC-features and features that quantify general stylistic properties such as average word length, number of emoticons and the like. Furthermore, we also experimented using only character or token n-grams to study their effectiveness in isolation.

Table 3 displays the results of these experiments. Using character and token n-grams in isolation hurts the accuracy of both gender and age prediction. But while the additional features do not aid age classification, they do yield significant advances for gender prediction. Additional experiments are needed to fully explore the spectrum of available features for these classification tasks.

Table 3. Effect of additional features for age and gender prediction. Results in bold indicate statistically significant results, as measured using approximate randomization testing.

	age	**gender**
Baseline: character + token n-grams	*76.7*	*68.8*
+ pos n-grams	**76.4**	**69.3**
+ PROFL-stylistic features	**76.2**	**69.5**
+ LIWC	76.7	**69.5**
+ sentiment	76.7	**69.8**
+ all of the above	**76.1**	**69.2**
only character n-grams	**76.4**	**66.2**
only token n-grams	**74.7**	**61.3**

5 CONCLUSION AND FUTURE WORK

We explored the capabilities of a text-based age and gender profiling system for application in a monitoring environment to secure the online safety of (young) social media users. More specifically, our research focused on the task of detecting sexual predators who try to "groom" children on social networking websites, often providing false age and/or gender information to get closer to their young targets. We presented results of age and gender prediction experiments on a dataset of almost 380,000 Dutch chat posts written by 86,610 users on the social networking platform Netlog.

The age prediction task was set up as a binary classification task, i.e. predicting whether an author is under or over a specific age. The age boundary that separates the two classes can be adapted to the specific use case at hand, based on legal constraints (e.g. the legal age of sexual consent) and age related statistics (e.g. grooming statistics). We carried out age prediction experiments with a range of different age boundaries and found that that macro-averaged F-scores improved as the age boundary increased. This effect persisted when we used data subsets that were balanced for age category and gender.

In addition, we presented a detailed analysis of the system's performance for authors of different ages, showing that classification errors were mainly concentrated around the age boundary. The consequences of our findings for the application were discussed, zooming in on the case study of detecting sexual offenders and their minor victims according to Belgium's current legal age of sexual consent, age 16. We found that practically usable recall and precision scores could be achieved for both the -16 and the 16+ classifier, especially when tuning the system towards a high recall. Furthermore, gender prediction, although not yielding high performance in our present experiments, can provide useful information when applied in addition to content analysis and age prediction.

[6] http://amicaproject.be/profl

In future research, we plan to further extend and optimize the feature set used for age and gender classification and extend our experiments to different datasets, including more recently collected chat data and other social media genres such as blog posts and tweets. We will also further test methods for high-recall tuning, including cost-sensitive learning techniques such as cost-proportionate rejection sampling [33]. In addition, we would like to study the applicability of linear regression for age prediction in the AMiCA system. In recent work, [20] produced encouraging results predicting author age on twitter using this technique. Finally, a crucial step is to test our profiling system on real-life sexual predator data, to investigate to what extent the method also works when people pretend to be someone of a different age and/or gender. In these tests, we will also add a text analysis component to detect sexual and grooming-related content in conversations.

ACKNOWLEDGMENTS

The research described in this paper was funded by IWT-SBO grant 120007 (AMiCA). We would like to thank Massive Media for providing the Netlog data.

REFERENCES

1. Peter Bach, Marjorie Glass Zauderer, Ayca Gucalp, Andrew S Epstein, Larry Norton, Andrew David Seidman, Aryeh Caroline, Alexander Grigorenko, Aleksandra Bartashnik, Isaac Wagner, Jeffrey Keesing, Martin Kohn, Franny Hsiao, Mark Megerian, Rick J Stevens, Jennifer Malin, John Whitney, Mark G. Kris. Beyond jeopardy!: Harnessing IBM's Watson to improve oncology decision making. *Journal of Clinical Oncology*, 31(suppl;abstract 6508), 2013.
2. Enric Junque de Fortuny, Tom De Smedt, David Martens, and Walter Daelemans. Media coverage in times of political crisis: A text mining approach. *Expert Systems with Applications*, 39(14):11616–11622, 2012.
3. Enric Junque de Fortuny, Tom De Smedt, David Martens, and Walter Daelemans. Evaluating and understanding text-based stock price prediction models. *Information Processing & Management*, 50(2):426–441, 2014.
4. Moshe Koppel, Shlomo Argamon, and Anat R. Shimoni. Automatically categorizing written texts by author gender. *Literary and Linguistic Computing*, 17:401–412, 2002.
5. James W Pennebaker and Lori D Stone. Words of wisdom: language use over the life span. *Journal of personality and social psychology*, 85(2):291–301, 2003.
6. Walter Daelemans. Explanation in computational stylometry. In Alexander Gelbukh, editor, *Computational Linguistics and Intelligent Text Processing, volume 7817 of Lecture Notes in Computer Science*, pages 451–462. Berlin, Heidelberg, 2013. Springer Berlin.
7. Giacomo Inches and Fabio Crestani. Overview of the international sexual predator identification competition at PAN-2012. In Pamela Forner and Jussi Karlgren and Christa Womser-Hacker, editors, *CLEF 2012 Evaluation Labs and Workshop – Working Notes Papers*, Rome, Italy, 2012. CLEF.
8. Francisco Rangel, Paolo Rosso, Moshe Koppel, Efstathios Stamatatos, and Giacomo Inches. Overview of the author profiling task at PAN-2013. In Pamela Forner, Roberto Navigli and Dan Tufis, editors, *CLEF 2013 Evaluation Labs and Workshop – Working Notes Papers*, pages 352–365, Valencia, Spain, 2013. CELCT.
9. Francisco Rangel, Paolo Rosso, Irina Chugur, Martin Potthast, Martin Trenkmann, Benno Stein, Ben Verhoeven, and Walter Daelemans. Overview of the 2nd author profiling task at PAN-2014. In Linda Cappellato and Nicola Ferro and Martin Halvey and Wessel Kraaij, editors, *CLEF 2014 Evaluation Labs and Workshop – Working Notes Papers*, pages 898–927, Sheffield, UK, 2014. CEUR-WS.org.
10. Francisco Rangel, Fabio Celli, Paolo Rosso, Martin Pottast, Benno Stein, Walter Daelemans. Overview of the 3rd Author Profiling Task at PAN 2015. In Linda Cappelato and Nicola Ferro and Gareth Jones and Eric San Juan, editors, *CLEF 2015 Labs and Workshops, Notebook Papers*, Toulouse, France, 2015. CEUR-WS.org
11. Bart Desmet and Veronique Hoste. Emotion detection in suicide notes. *Expert Systems With Applications*, 40(16):6351–6358, 2013.
12. Cynthia Van Hee, Ben Verhoeven, Julie Mennes, Els Lefever, Bart Desmet, Guy De Pauw, Walter Daelemans, and Veronique Hoste. Detection and fine-grained classification of cyberbullying events. In Galia Angelova and Kalina Bontcheva and Ruslan Mitkov, editors, *Proceedings of the 10th Recent Advances in Natural Language Processing*, pages 672–680, Hissar, Bulgaria, 2015. Association for Computational Linguistics
13. Claudia Peersman, Walter Daelemans, and Leona Van Vaerenbergh. Predicting age and gender in online social networks. In *Proceedings of the 3rd International Workshop on Search and Mining User-generated Contents*, pages 37–44, New York, USA, 2011. ACM.
14. Jonathan Schler, Moshe Koppel, Shlomo Argamon, and James W Pennebaker. Effects of age and gender on blogging. In *Computational Approaches to Analyzing Weblogs, Papers from the 2006 AAAI Spring Symposium*, pages 199–205, Menlo Park, USA, 2006. The AAAI Press.

15. Shlomo Argamon, Moshe Koppel, James W Pennbaker, and Jonathan Schler. Automatically profiling the author of an anonymous text. *Communications of the ACM*, 52(2):119–123, 2009.
16. Cathy Zhang and Pengyu Zhang. Predicting gender from blog posts. Technical report, University of Massachusetts Amherst, USA, 2010.
17. Arjun Mukherjee and Bing Liu. Improving gender classification of blog authors. In Jun'ichi Tsujii and James Henderson and Marius Pasca, editors, *Proceedings of the 2010 Conference on Empirical Methods in Natural Language Processing*, pages 207–217, Cambridge, MA, 2010. Association for Computational Linguistics.
18. Delip Rao, David Yarowsky, Abhishek Shreevats, and Manaswi Gupta. Classifying latent user attributes in Twitter. In *Proceedings of the 2nd International Workshop on Search and Mining User-generated Contents*, pages 37–44, New York, USA, 2010. ACM.
19. Shane Bergsma and Benjamin Van Durme. Using conceptual class attributes to characterize social media users. In Pascale Fung and Massimo Poesio, editors, *Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics* (Volume 1: Long Papers), pages 710–720, Sofia, Bulgaria, 2013. Association for Computational Linguistics.
20. Dong Nguyen, Rilana Gravel, Dolf Trieschnigg, and Theo Meder. "How Old Do You Think I Am?"; A Study of Language and Age in Twitter. In *Proceedings of the Seventh International AAAI Conference on Weblogs and Social Media*, pages 439–448, Cambridge, USA, 2013. AAAI Press.
21. David Bamman, Jacob Eisenstein, and Tyler Schnoebelen. Gender identity and lexical variation in social media. *Journal of Sociolinguistics*, 18(2):135–160, 2014.
22. Katja Filippova. User demographics and language in an implicit social network. In Jun'ichi Tsujii and James Henderson and Marius Pasca, editors, *Proceedings of the 2012 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning*, pages 1478–1488, Jeju Island, Korea, 2012. Association for Computational Linguistics.
23. John D. Burger and John C. Henderson. An exploration of observable features related to blogger age. In *Computational Approaches to Analyzing Weblogs, Papers from the 2006 AAAI Spring Symposium*, pages 15–20, Menlo Park, USA, 2006. The AAAI Press.
24. Faiyaz Al Zamal, Wendy Liu, and Derek Ruths. Homophily and latent attribute inference: Inferring latent attributes of Twitter users from neighbors. In *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media*, pages 387–390, Palo Alto, USA, 2012. The AAAI Press.
25. Xiang Yan and Ling Yan. Gender classification of weblog authors. In *Computational Approaches to Analyzing Weblogs, Papers from the 2006 AAAI Spring Symposium*, pages 228–230, Menlo Park, USA, 2006. The AAAI Press.
26. Shigeyuki Sakaki, Yasuhide Miura, Xiaojun Ma, Keigo Hattori, and Tomoko Ohkuma. Twitter user gender inference using combined analysis of text and image processing. In *Proceedings of the Third Workshop on Vision and Language*, pages 54–61, 2014. Dublin City University and the Association for Computational Linguistics
27. Nikesh Garera and David Yarowsky. Modeling latent biographic attributes in conversational genres. In Keh-Yih Su and Jian Su and Janyce Wiebe and Haizhou Li, editors, *Proceedings of the Joint Conference of the 47th Annual Meeting of the ACL and the 4th International Joint Conference on Natural Language Processing of the AFNLP*, pages 710–718, Suntec, Singapore, 2009. Association for Computational Linguistics.
28. Sara Rosenthal and Kathleen McKeown. Age prediction in blogs: A study of style, content, and online behavior in pre- and post-social media generations. In Yuji Matsumoto and Rada Mihalcea, editors, *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies*, pages 763–772, Portland, USA, 2011. Association for Computational Linguistics.
29. Sarah Schulz, Guy De Pauw, Orphee De Clercq, Véronique Hoste Bart Desmet, Walter Daelemans, and Lieve Macken. Multi-modular text normalization of dutch user-generated content. *ACM Transactions on Intelligent Systems and Technology*, 2016 (in press).
30. Fabian Pedregosa, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg, Jake Vanderplas, Alexandre Passos, David Cournapeau, Matthieu Brucher, Matthieu Perrot, Édouard Duchesnay. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12:2825–2830, 2011.
31. John D. Burger, John Henderson, George Kim, and Guido Zarrella. Discriminating gender on Twitter. In David Yarowsky and Timothy Baldwin and Anna Korhonen and Karen Livescu and Steven Bethard, editors, *Proceedings of the Conference on Empirical Methods in Natural Language Processing*, EMNLP '11, pages 1301–1309, Stroudsburg, USA, 2011. Association for Computational Linguistics.
32. Ruchita Sarawgi, Kailash Gajulapalli, and Yejin Choi. Gender attribution: Tracing stylometric evidence beyond topic and genre. In Sharon Goldwater and Christopher Manning, editors, *Proceedings of the Fifteenth Conference on Computational Natural Language Learning*, pages 78–86, Portland, USA, June 2011. Association for Computational Linguistics.
33. Bianca Zadrozny, John Langford, and Naoki Abe. Cost-sensitive learning by cost-proportionate example weighting. In *Proceedings of the Third IEEE International Conference on Data Mining*, ICDM '03, pages

435–442, Washington, USA, 2003. IEEE Computer Society.

ISSN: 2305-0012 (online)

International Journal of
Cyber-Security and Digital Forensics

2016

- The main objectives of this journal with regard to security, privacy, digital forensics, hacking, and cyber warfare are as follows:

- **Encouraging the study, improve the practice, and advance the knowledge;**
- **Providing the intended audiences with the latest advancements;**
- **Transferring the knowledge;**
- **Closing the gap between academia and the industry;**
- **Providing trusted source of knowledge;**
- **Encouraging talents and innovations;**
- **Supporting collaboration and communication;**
- **Encouraging the applied research.**

The IJCSDF scope covers the following areas (but not limited to): cyber security, computer forensics, privacy, trust, hacking techniques, cyber warfare, cryptography, cybercrime, cyber-terrorism, cryptography, formal methods application in security and forensics, data piracy, database security and forensics, wired and wireless network security and investigation, mobile network security and forensics, incident handling, malware forensics and steganography.

- The IJCSDF is published four (4) times a year and accepts three types of papers as follows:

Research papers: that are presenting and discussing the latest, and the most profound research results in the scope of IJCSDF. Papers should describe new contributions in the scope of IJCSDF and support claims of novelty with citations to the relevant literature. Maximum word limit of 8000!

Technical papers: that are establishing meaningful forum between practitioners and researchers with useful solutions in various fields of digital security and forensics. It includes all kinds of practical applications, which covers principles, projects, missions, techniques, tools, methods, processes etc. Maximum word limit of 5000

Review papers: that are critically analyzing past and current research trends in the field. Maximum word limit of 12000!

Book reviews: providing critical review of a recently published book in the scope of IJCSDF. Maximum word limit of 1000!

ISSN: 2305-0012 (online)

International Journal of
Cyber-Security and Digital Forensics

2016

Volume 5, Issue 1

CONTENTS

ORIGINAL ARTICLES

International Journal of Cyber Security and Digital Forensics

(IJCSDF)
ISSN 2305-0012

Volume 5, Issue 1
2016

SDIWC
www.sdiwc.net