ABSTRACT

In recent years, Online Social Network (OSN) is a popular and efficient medium to facilitate a high degree of user personalization and user intercommunication. The enormous growth of OSN has also resulted in an increase of significant criminal activities including identity theft, piracy, illegal trading, cyber stalking and cyberterrorism. Cyber criminals are becoming increasingly sophisticated in attempting to use social networking based technology in order to evade detection and perform criminal acts. This happens in virtual environment using social network as a communication medium and it gives fraudsters an increased chance of attacking systems. In addition, combating this growing level of crime is challenging due to the ever increasing scale of today's OSN.

A newly proposed social network threat, called Stegobot, masks crucial information in a digital image by using a technique known as steganography. Stegobot works by hiding malicious codes inside any image, uploads it into infected users profile and then waits for the new users profile and then waits for the new user to look at the infected user profile. In this way, another user is also infected and sensitive information related to the user can be stolen easily by the botmaster.

The botmaster can also send commands to the bots through the reverse process by uploading an image with hidden instructions that makes way to infect computers. Criminals could employ Stegobot for their secret communication, as it is hard to detect because of the probabilistically

unobservable communication channels connecting the bots and botmaster. However, the existing steganalysis algorithms find it difficult to detect Stegobot when applied to the heterogeneous image sources under the practical social network environment. The social network consists of images generated by various profile users equipped with different image quality, image based bot binaries, image malware and various social network related activities. This new social network threat motivates us to design new efficient forensics aided steganalysis based detection mechanisms against such botnets.

Approaches to the steganalysis problem depend heavily on the steganographic security model, and particularly on the steganalyst's knowledge about the cover source and the behavior of opponent. The most studied steganalysis models are quite far from detection of Stegobot communication channel, and it is clear that state of the art steganalysis could not yet be used effectively in the detection of Stegobot. Since Stegobot profiles in OSN look like genuine profile, these approaches cannot detect new kind of bots. Due to these difficulties, it would be desirable to develop additional methodologies to overcome these issues.

The contribution of this thesis is threefold. Two chapters deal with the problem from steganalysis point of view. We introduce a new universal steganalysis based on the contourlet transform which uses the properties of contourlet transform to detect stego images and botcargo and to classify the normal and Stegobot communications. The important aspect of this work is that it uses the minimum number of features in the transform domain and gives better accuracy while classifying normal and stego images. In the next

work, we introduce coding theory based steganalysis against BCH code based stegosystem which offers very smart solution based on the hardness of syndrome decoding problem. This approach provides a different flavor from classical steganalysis techniques which are using thresholds or learning model to infer stego objects. This scheme also estimates the number of bit changes in the cover image and finds their locations.

The second approach for the detection of Stegobot is based on machine learning techniques with significant features related to the profiles in social network. In this research work, we propose an effective method to detect Stegobot hosts within a monitored social network. Based on the observations, Stegobot often has a differentiable communication pattern because of its unique design and implementation. Hence by investigating each host profile activity, it is possible to determine whether the profile is a Stegobot or normal. Further we extend this method to detect the Stegobot communications between the profiles in social network community. Composition of image steganographic features, social network features and graph theoretic features are used to identify profiles that experience a sudden change in behavior. Also our study shows that some of the identified attributes are significant for classification of data and can be useful for a network forensic analyst to develop better prevention strategies. We apply the proposed method on four popular social networking sites Facebook, Flickr, Twitter and Google+.

The next approach is using epidemic models. In this work, behavior of social network profiles is analyzed and Stegobot propagation is modeled by

epidemic models. This model addresses the dynamic characteristics of Stegobot more accurately. Bot-free equilibrium, epidemic equilibrium and basic reproduction numbers are obtained theoretically. The proposed model is evaluated with datasets like Facebook, Flickr, Barracude lab. Using reproduction number one can analyze the growth of Stegobot.

In this research work, a detailed study and analysis of Stegobot is carried out. Different techniques are proposed to detect Stegobot at image level, profile level and communication level. These investigations and methods could ultimately be useful to network security researchers as well. In future, large scale infiltration in OSNs is a major cyber threat and defending against such threat is a challenge. This research would be the first step towards maintain a secure and safer multimedia social network for millions of users.