IMG-GUARD: Watermark Based Approach for Image Privacy in OSN Framework

Rishvinbanu E
Computer Science and Engineering
University College of Engineering
Thirukkuvalai
rishvinbanu@gmail.com

Sujitha T
Computer Science and Engineering
University College of Engineering
Thirukkuvalai
sujithat1996@gmail.com

Subathra R
Computer Science and Engineering
University College of Engineering
Thirukkuvalai
subathrakrish25@gmail.com

Gopikrishnan R
Department of Computer Science and Engineering
University College of Engineering
Thirukuvalai
gopikrish.cse@gmail.com

ABSTRACT: A social networking service (also social networking site, SNS or social media) is an online platform that is used by people to build social networks or social relations with another persons who are share their own details or career interests, activities, backgrounds or real-life connections. Social networking sites are varied and they incorporate a range of new information and various tools such as availability personal computers, mobile devices such as tablet computers and smart phones, digital photo/video/sharing and "web logging" diary entries online (blogging). While Online Social Networks (OSNs) enable users to share photos easily, they also expose users to several privacy threats from both the OSNs and external entities. The current privacy controls on social networks are far from adequate, resulting in inappropriate flows of information when users fail to understand their privacy settings or OSNs fail to implement policies correctly. Social networks may be complicated because of privacy expectations when they reserve the right to analyze uploaded photos using automated watermarking technique. A user who uploads digital data such as image to their home page may wish to share it with only mutual friends, which OSNs partially satisfy with privacy settings. In this paper, we concentrate to solve the privacy violation problem occurred when images are published on the online social networks without the permission. According to such images are always shared after uploading process. Therefore, the digital image watermarking based on DWT co-efficient. Watermark bits are embedded in uploaded images. Watermarked images are shared in user homages can be difficult to misuse by other persons.

*****

I. INTRODUCTION:

A social networking service (also social networking site, SNS or social media) is an online platform that is used by people to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections. The variety of stand-alone and built-in social networking services currently available in the online space introduces challenges of definition; however, there are some common features: (1) social networking services are Web 2.0 internet-based applications (2) user-generated content (UGC) is the lifeblood of SNS organisms, (3) users create service-specific profiles for the site or app that are designed and maintained by the SNS organization, and (4) social networking services facilitate the development of online social networks by connecting a user's profile with those of other individuals and/or groups. Most social network services are web-based and provide means for users to interact over the Internet, such as by e-mail and instant messaging and online forums. Social networking sites are varied and they incorporate a range of new information and communication tools such as availability on desktop and laptops, mobile devices such as tablet computers and smartphones, digital photo/video/sharing and "web logging" diary entries online (blogging). Online community services are sometimes considered a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, digital photos and videos, posts, and inform others about online or real world activities and events with people in their network. While in-person social networking, such as gathering in a village market to talk about events has existed since the earliest developments of towns, the Web enables people to connect with others who live in different locations,

ranging from across a city to across the world. Depending on the social media platform, members may be able to contact any other member. In other cases, members can contact anyone they have a connection to, and subsequently anyone that contact has a connection to, and so on. LinkedIn, a career social networking service, generally requires that a member personally know another member in real life before they contact them online. Some services require members to have a preexisting connection to contact other members.

The main types of social networking services are those that contain category places (such as former school year or classmates), means to connect with friends (usually with self-description pages), and a recommendation system linked to trust. Social network services can be split into three types: socializing social network services are primarily for socializing with existing friends (e.g., Facebook); networking social network services are primarily for non-social interpersonal communication (e.g., LinkedIn, a career and employment-oriented site); and social navigation social network services are primarily for helping users to find specific information or resources. There have been attempts to standardize these services to avoid the need to duplicate entries of friends and interests.

Online Social Networks (OSNs) have become part of daily life for millions of users. Users building explicit networks that represent their social relationships and often share a wealth of personal information to their own benefit. The potential privacy risks of such behavior are often underestimated or ignored. The problem is exacerbated by lacking experience and awareness in users, as well as poorly designed tools for privacy-management on the part of the OSN. Furthermore, the centralized nature of OSNs makes users dependent and puts the Service Provider in a position of power. Because Service Providers are not by definition trusted or trustworthy, their practices need to be taken into account when considering privacy risks. Aside from allowing users to create a network to represent their social ties, many OSNs facilitate uploading of multimedia content, various ways of communication and sharing many aspects of daily life with friends. People can stay in touch with (physically remote) friends, easily share content and experiences and stay up to date in the comfort of their own home or when on the move. However, benefits aside, potential threats to user privacy are often underestimated. For example, due to the public nature of many OSNs and the Internet itself content can easily be disclosed to a wider audience than the user intended. Users often have trouble revoking or deleting information, and information about a user might even be posted by others without their consent. Privacy in OSNs is a complicated matter and is not always intuitive to users, especially because it is not always similar to how privacy works in real-life interactions.

II. RELATED WORKS:

2.1 Title: A Provably Secure Anonymous Buyer–Seller Watermarking Protocol

Author: Alfredo Rial Year: 2010

Encryption and digital watermarking are recognized as promising techniques for copyright protection. Encryption prevents unauthorized access to digital content. The limitation is that, once the content is decrypted, it does not prevent illegal replications by an authorized user. Digital watermarking is a technique that allows some information to be embedded into a digital content. As an application of watermarking, fingerprinting can be used to identify the content and to associate it to a customer. The fingerprint can be either an intrinsic feature of the content or some external information embedded into the content. At algorithmic level, watermarking is the function that embeds this information, while fingerprinting refers to the complete protocol between seller and buyer. Traditional watermarking-based fingerprinting schemes assume that content providers are trustworthy that they would never distribute content illegally and always perform the watermark embedding honestly. However, in practice, such assumptions are not fully established. This problem was first identified as the customer's rights problem, where the watermark is generated and embedded solely by the content provider (or the seller). A customer (or a buyer) whose watermark has been found in unauthorized copies can claim that the pirated copy was created by the seller. This could be done, for instance, by a malicious seller who may be interested in framing the buyer. It could be also possible when the seller is not the original owner but a reselling agent who could potentially benefit from making unauthorized copies. Finally, even if the seller was not malicious, an unauthorized copy containing the buyer's fingerprint could have originated from a security breach in the seller's system but not from the buyer. The main contribution of work is a formal security analysis of BSW protocols. We employ the ideal-world/real-world paradigm to define security of anonymous BSW protocols. Additionally, we define security for blind and readable watermarking schemes, and analyze the properties that watermarking schemes should provide for the construction of secure BSW protocols.

2.2 Title: Markov process-based retrieval for encrypted JPEG images

Author: Hang Cheng Year: 2016

Consider a privacy-preserving image retrieval scheme which involves three parties: content owner, authorized user, and server. The content owner encrypts images in the JPEG format and then stores them into cloud servers. The authorized user, may be a content owner, has desire to retrieval images similar to the encrypted query image from

encrypted database images. When receiving the encrypted query image, the server can calculate the distances between the encrypted query image and database images and then returns encrypted images similar to the query image in plaintext content, without knowing anything about the plaintext contents of the involved encrypted images. It is known that there exist the intra-block, inter-block, and inter-component dependencies among DCT coefficients of a color JPEG image. Moreover, in some sense, the three types of dependencies are similar between similar images. Based on the analysis, propose a novel scheme for encrypted JPEG images, where intra-block, inter-block, and inter-component dependencies among DCT coefficients are introduced. With this scheme, the encrypted JPEG images can be obtained through a combination of the stream cipher and permutation encryption and outsourced to a server. And also, with the given encrypted query image and the encrypted database images, it is easy for the server to calculate their similarities in encrypted domain by employing the techniques of a Markov process and multi-class support vector machine (SVM). As the purpose of scheme is to address the problem of image retrieval in encrypted domain while preserving the file size and format compliance for JPEG images, here, first take a partial image encryption technique into account to encrypt JPEG images. The problem is difficult to solve for the traditional cryptography. The most existing partial encryption techniques for JPEG images are mainly based on blocks shuffle, DCT coefficient permutation,
and encrypting the signs of DCT coefficients. Recent work presents a novel partial encryption method based on a JPEG bit-stream, which aims to implement reversible data hiding in an encrypted gray JPEG image. The proposed encryption method cannot only meet the requirements of format compliance and file size preservation but also provide valuable information regarding the length of each variable length integer (VLI) code for DCT coefficients. More importantly, the encryption method can make the length of each VLI code remain unchanged before and after encryption.

2.3 Title: Secure an image Retrieval Based on Visual Content and Watermarking Protocol
Author: Jun Zhang, Year 2011

First, the participants and their roles in an image retrieval watermarking protocol are different from those in a buyer–seller watermarking protocol. In a buyer– seller watermarking protocol, the seller is the owner of a digital content, who conducts the watermark insertion, and the buyer can obtain a watermarked digital content. In contrast, in an image-retrieval watermarking protocol, the user is the owner of a query image, who should insert a watermark to protect its right, and the service provider of CBIR will search images according to the watermarked query image obtained from the user. The difference makes some existing security solutions inapplicable; e.g. the solution of the unbinding problem for a buyer–seller watermarking protocol is inapplicable in an image-retrieval watermarking protocol. Second, a new watermarking protocol should be easily embedded in real-world image retrieval systems. It should require a direct interaction between the user and the service provider. In the previous work, a three-party protocol was proposed to solve the user right problem in CBIR systems. However, that protocol is based on a trusted third party, WCA, and the user needs to contact WCA for requesting a watermark, which is against the user's habits in CBIR and will hinder the applications of CBIR. In this paper, a novel two-party watermarking protocol is proposed to overcome this shortcoming. The proposed protocol provides a higher security level by solving the problems that were not considered in the previous work. Third, different watermarking protocols have different requirements to balance the quality of watermarked digital content and the robustness of digital watermark. It is a hard problem behind buyer–seller watermarking protocols, since the customer requires high-quality digital content, which conflicts with the the robustness of digital watermark. However, this problem is not serious in the CBIR systems, because the user cares about the retrieval performance instead of the quality of watermarked query image. In this paper, a novel research on content-based image retrieval of watermarked query images is reported to show that it is possible to improve the robustness of digital watermark by reducing the quality of watermarked query images without influencing retrieval performance. This problem has two aspects. On the one hand, the service provider of CBIR may distribute the user's private query image without authentication. On the other hand, the user may frame a service provider.

2.4 Title: Secure Watermarking for Multimedia Content Protection
Author: Tiziano Bianchi Year 2013

To tackle the problem of watermark detection in the presence of an untrusted verifier (to whom watermark secrets cannot be disclosed), a possible solution offered by secure signal processing is represented by zero-knowledge watermark detection (ZKWD) that uses a cryptographic protocol to wrap a standard watermark detection process. In general, a ZKWD algorithm is an interactive proof system where a prover tries to convince a verifier that a digital content x is watermarked with a given watermark b without disclosing b. In contrast to the standard watermark detector, in ZKWD the Verifier is given only properly encoded (or encrypted) versions of security-critical watermark parameters. Depending on the particular protocol, the watermark code, the watermarked object, a watermark key or even the original unmarked object is available in an

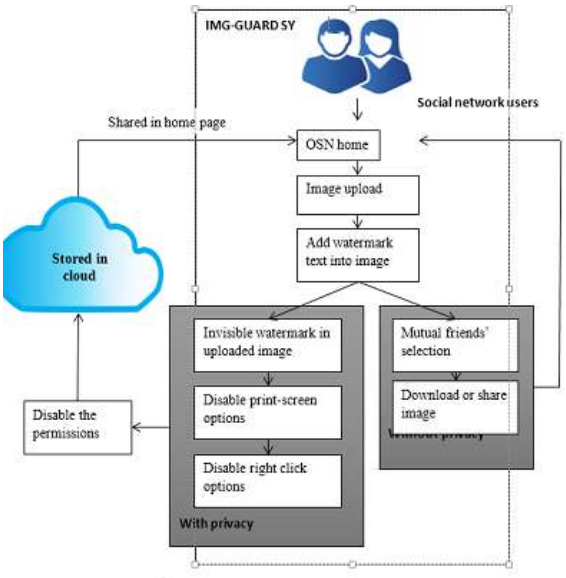
encrypted form to the verifier. The Prover runs the zero-knowledge watermark detector to demonstrate to the Verifier that the encoded watermark is present in the object in question, without removing the encoding. A protocol run will not leak any information except for the unencoded inputs and the watermark presence detection result. A flexible solution for zero-knowledge watermark detection is to compute the watermark detection statistic in the encrypted domain (e.g., by using additive homomorphic public-key encryption schemes or commitments) and then use zero-knowledge proofs to convince the Verifier that the detection statistic exceeds a fixed threshold. Apart from the foreseeable evolution of the hardware equipment or advancements in homomorphic encryption, an appealing solution from a signal processing point of view could be combining these schemes with partial encryption techniques, which are often employed in video encryption. In closely related fields, partial encryption has been employed in secure client-side watermarking and as a means for implementing commutative watermarking and encryption. The rationale behind such an approach is that signals are fuzzy entities, which do not require complete protection, so that we can trade off security for a better efficiency. Client-Side Asymmetric Fingerprinting: Although client-side embedding provides an elegant solution to the system scalability problem, the incorporation of the aforementioned technique in an asymmetric fingerprinting protocol does not appear an easy task.

2.5 Title: Secure Client-Side ST-DM Watermark EmbeddingAuthor: Alessandro Piva Year: 2010

An alternative solution is represented by the client-side watermark embedding: in this case, a server–client architecture is again adopted; however, in this case, the server is allowed to send a unique copy of the content to all the interested users through broadcasting systems, without the need to generate different watermarked copies (thus removing the bottlenecks present in the server-side watermark embedding approach); instead, each client will be in charge of embedding a personal watermark identifying the received copy. In this case, however, since the clients are untrusted, proper solutions need to be devised not to allow malevolent users to have access to the original content or to the watermark to be inserted. A new approach, defined as secure watermark embedding, has been proposed for facing such a problem: here, the server transmits the same encrypted version of the original work to all the clients, but a client-specific secret allows decryption of the content and at the same time implicit embedding of a personalized watermark, obtaining a uniquely watermarked version of the work. To move one step further in the field of secure client-side watermark embedding for multimedia content distribution, considered to improve the above-mentioned method through the adoption of a more robust watermarking scheme. By relying on the well-known results coming from the watermarking community on the superiority of the class of informed embedding (or host-interference rejecting) data hiding schemes with respect to the classical SS methods, aim was to modify the model proposed so that the secure client-side embedding scheme will be able to embed a watermark belonging to the quantization index modulation (QIM) class, that has rapidly become popular as one of the best performing watermarking strategies. In particular, we properly designed an LUT-based secure client-side embedding system allowing us to embed a spread transform dither modulation (ST-DM) watermark. As it will be demonstrated in the following sections, this modification is not straightforward, since the client-side embedding framework imposes some constraints that do not allow us to embed a pure ST-DM watermark. Still, the experimental results will confirm that the superiority of ST-DM versus SS watermarking exhibited in the classical embedding schemes is maintained also in the client-side embedding approach. First, we computed the perceptual degradation introduced by the two watermarking systems, to verify if a comparison between them with equivalent DWR is fair also from the point of view of perceptual quality.

III. SYSTEM DESIGN:

5.1 SYSTEM ARCHITECTURE:



IV. SYSTEM IMPLEMENTATION:

6.1 MODULES:

Social network creation
Upload image
Embed the watermark
Privacy settings
Protection system

6.2 MODULES DESCRIPTION:

6.2.1 Social network creation:

Social network refers to interaction among people in which they create, share, and/or exchange information and ideas in virtual communities and networks. A social network manager is the individual in an organization trusted with monitoring, contributing to, and filtering, measuring and otherwise guiding the social media presence of a brand, product, individual or corporation. In face book,GUI is a type of user interface that allows users to interact with users through graphical icons and visual indicators such as secondary notation, as opposed to text-based interfaces, typed command labels or text navigation. In this module, we can have three types of users such as image owner, image users and image server. Image owner can be upload the image into system and image server stores the images in database. Image users use images which are shared by image owner.

6.2.2 Upload image:

The first stage of any sharing system is the image acquisition stage. After the image has been obtained, various methods of processing can be applied to the image to perform the many different vision tasks required today. However, if the image has not been acquired satisfactorily then the intended tasks may not be achievable, even with the aid of some form of image enhancement. The basic two-dimensional image is a monochrome (greyscale) image which has been digitized. Describe image as a two-dimensional light intensity function f(x,y) where x and y are spatial coordinates and the value of f at any point (x, y) is proportional to the brightness or grey value of the image at that point. In this module, we can upload various images such as natural images, face images and other images. Uploaded images can by any type and any size.

6.2.3 Embed the watermark:

In this module, we can embed the watermark text into images. Digital media can be stored efficiently and can be manipulated very easily using computers, resulting in various security issues. The problem of protecting the copyright of digital media can be solved by digital watermark. Digital watermarking is a concept of hiding ownership data into the multimedia data, which can be extracted later on to prove the authenticated owner of the media. Watermarking ensures authenticating ownership, protecting hidden information, prevents unauthorized copying and distribution of images over the internet and ensures that a digital picture has not been altered. We can implement Discrete Wavelet Transform (DWT) domain image watermarking system for real time image. In the embedding process, the watermark may be encoded into the cover image using a specific location. This location values is used to protect the images. The output of the embedding process, the watermarked image, is then transmitted to the OSN home page.

6.2.4 Privacy settings:

Each user images are first categorized into privacy policy. Then privacy policies of each images can be categorized and analyzed for predict the policy. So we adopting two stages approach for policy recommendation than applying the common one-stage data mining approaches to mine both image features and policies together. The two-stage approach allows the system to employ the first stage to classify the policy as with privacy or without privacy. In the second stage, we can set without privacy means, prefer the user list details.

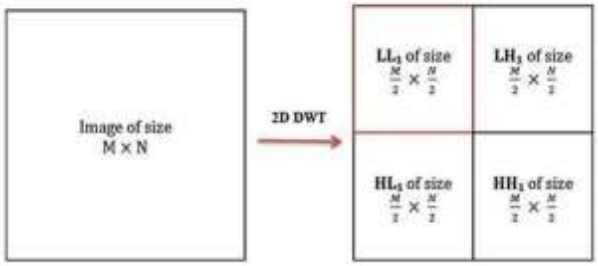
6.2.5 Protection system:

In this module, we can set the protection or blocking system to avoid third party aces without knowledge of image owners. This module is used to set the image with privacy. If user set with privacy settings means, all users are considered as third parties. Based on this setting, unauthorized user only views the image and can't be used. If he downloads means, only get water mark values. Finally provide hardware control system such as mouse controls and keyboard controls. Then disable the mouse operations and system print screen options. Mouse code and print screen controls values are extracted and to provide coding implementation to disable the coding as false settings. We can implement this concept in all browsers and to implement in all images which are shared by social users.

V. ALGORITHM AND TECHNIQUES:

7.1 DISCRETE WAVELET TRANSFORM:

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchical decomposition of an image. The transformation is based on decomposing a signal into wavelets or small waves, having varying frequency and limited duration. The properties of wavelet decompose an original signal into wavelet transform coefficients which contains the position information. The original signal can be reconstructed completely by performing Inverse Wavelet Transformation on these coefficients. DWT decomposes an image into sub images or sub bands, three details and one approximation. The bands are LL, LH, HL and HH.



The figure shows the sub bands in DWT. LL contains low frequencies both in horizontal and vertical direction. HH contains high frequencies both in horizontal and vertical direction. HL contains high frequencies in horizontal direction and low frequencies in vertical direction. LH contains low frequencies in horizontal direction and high frequencies in vertical direction. The low frequency part comprises of the coarse information of the signal while high frequency part comprises of the information related to the edge components. The LL band is the most significant band as it contains most of the image energy and represents the approximations of the image. Watermarks can be embedded in the high frequency detail bands (LH, HL and HH) as these regions are less sensitive to human vision. Embedding into these bands increases the robustness of the watermark without having additional impact on the quality of the image. At each level of decomposition, first DWT is performed in the vertical direction, followed by the DWT in the horizontal direction. The first level of decomposition yields four subbands: LL1, LH1, HL1, and HH1. The LL sub band of the previous level is used as the input for every successive level of decomposition. This LL sub-band is further decomposed into four multi resolution sub-bands to acquire next coarser wavelet coefficients. This process is repeated several times based on the application for which it is used. DWT has excellent spatio-frequency localization property that has been extensively utilized to identify the image areas where a disturbance can be more easily hidden. Also this technique does not require the original image for watermark detection. Digital image watermarking consists of two processes first embedding the watermark with the information and second extraction.

Watermark Embedding:

In this process 2D DWT is performed on the cover image that decomposes the image into four sub-bands: low frequency approximation, high frequency diagonal, low frequency horizontal and low frequency vertical sub- bands. Similarly 2D DWT is performed on the watermark image that has to be embedded into the cover image. Here we have used Haar wavelet. The technique used for inserting watermark is alpha blending. The decomposed components of cover image and watermark are further multiplied by a particular scaling factor and are added. During the embedding process the size of the watermark should be smaller than the cover image but the frame size of both the images should be made equal. The watermark embedded in this paper is perceptible or visible in nature, so we embedded it in the low frequency approximation component of the cover image.

Watermark Extraction

In this process the steps applied in the embedding process are applied in the reverse manner. First discrete wavelet transform is applied to both cover image and the watermarked image. After this the watermark is recovered from the watermarked image by using inverse discrete wavelet transform.

VI. CONCLUSION AND FUTURE ENHANCEMENT

8.1 CONCLUSION:

The appearance of well-known online social networking has triggered within the compromise of conventional notions of privateness, certainly in visual media. With a view to facilitate useful and principled protection of picture privateness online, we have got supplied the design, implementation, and evaluation of photo shield gadget that successfully and successfully protects client's photo privateness across famous OSNs. The digital watermarking approach based fully on DWT coefficients modification for social networking offerings has been presented on this paper. In the embedding manner, the coefficients in LL sub-band had been used to embed watermark. Within the extraction process, normal coefficient prediction based on imply clear out is used to boom the accuracy of the extracted watermark. On extending the Machine Learning (ML) text categorization techniques to automatically assign with each short text message a set of categories based on its content. Then exploiting a flexible language to specify Filtering Rules (FRs), by which users can state what contents, should not be displayed on their walls. FRs can support a variety of different filtering criteria that can be combined and customized according to the user needs.As part of future work, to implement cryptographic techniques and various filtering techniques to secure OSN home page. And also extend the work in privacy based uploaded video content sharing sites. The experimental outcome confirmed a larger overall efficiency in specific time application.

8.2 FUTURE ENHANCEMENT:

In future, we can extend the work to implement image privacy with hardware system. We can implement sensors to block the various mobile snapshots and implement message privacy with various languages with accuracy rate.

REFERENCES:

[1] H. Cheng, X. Zhang, J. Yu, and F. Li, "Markov process based retrieval for encrypted jpeg images," in Proc. of 10th International Conference on Availability, Reliability and Security. IEEE, 2015, pp. 417–421.

[2] A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, "A provably secure anonymous buyer–seller watermarking protocol," Information Forensics and Security, IEEE Transactions on, vol. 5, no. 4, pp. 920–931, 2010.

[3] J. Zhang, Y. Xiang, W. Zhou, L. Ye, and Y. Mu, "Secure image retrieval based on visual content and watermarking protocol," The Computer Journal, vol. 54, no. 10, pp. 1661–1674, 2011.

[4] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 87–96, 2013.

[5] A. Piva, T. Bianchi, and A. De Rosa, "Secure client-side st-dm watermark embedding," Information Forensics and Security, IEEE Transactions on, vol. 5, no. 1, pp. 13–26, 2010.

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt. Springer, 2004, pp. 506–522.

[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy. IEEE, 2000, pp. 44–55.

[8] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[10] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," Journal of Internet Technology, vol. 16, no. 1, pp. 171–178, 2015.