Abstract

Purpose; Cyber sexual violence is a sexual crime deriving from information and communication technology such as the Internet and digital devices including camera and has become a serious social issue. The government has enacted various legislations and eradicative measures, yet the spread of cyber sexual crime images and its re-distribution are not eliminated, but constantly increasing. Hence, this study would propose a Webhard Monitoring System.

The proposal Webhard Monitoring system stores extracted features from cyber sexual violence images in database, utilize the stored data for various techniques such as Text-based, Content-based and Semantic-based retrievals. When any image with high index of similarity with the crime image is retrieved, the image is downloaded and checked, and then notify the webhard. The webhard with the retrieval result reception blocks any access to the crime image and transfer the personal information of the image uploader to identification information monitoring system. The system stores and manages the original crime piece and uploader personal information received from the webhard and characteristics of the image for further monitoring processes.

This proposes a monitoring system to rapidly and accurately monitor webhards. The proposal webhard monitoring system retrieves and deletes cyber sexual crime image to prevent re-distribution, and even allows tracking the first distributor of the crime image in the webhards. Considering the characteristics of cyber sexual violence – unavailability of victims to recognize their damage and time-consuming cost to recognize the damage – immediate blocking and deleting the cyber sexual violence image is urgently necessary regardless of the request by victims.

[Keywords] Cyber Sexual Violence, Monitoring, Webhard, Text Based, Content Based, Semantic Based

1. Introduction

Cyber-crime refers to illegal commitments and various crimes such as hacking, illegal use of information and spread of malignant programs in the process of information acquisition within cyberspace[1]. Untact, Expertise, Technology, Unrestricted Time and Space, Anonymity, Repeatability, Continuity and Rapid Dissemination of cyber-crimes characterize high degrees of damage and hidden crimes[2]. Cyber sexual violence, the most severe crime among cyber-crimes, is a crime infringing on sexual self-determination without any direct relationship, face-to-face and physical contact. Moreover, expropriating and manipulating sexual images of a random person and threatening, sexual harassment, forceful solicit for prostitution and other derivative crimes via using sexual images are commonly called cyber sexual violence[3].
Recent technology development has allowed the release of hidden cameras in forms of daily necessities with high smartphone camera performance and capacities of high-resolution images and images. Using these filming equipment, cyber sexual violence, spreading various sexual crime images, which sneaked women bodies in public places such as subway stations and terminals via hidden cameras in toilets and fitting rooms and filmed sexual relations, in webhard, chatting and SNS, has become a serious issue[4].

Cyber sexual violence images have not often resulted in a complete prevention of further spread even after the suspect arrests. According to private data deletion companies, the number of cyber sexual crime images being spread in general on the Internet is assumed approximately 100 thousand cases, and the actual number of cyber sexual crime images requesting webhards for its deletion and block has reached 300 thousand cases[3]. The cause of such circumstance is due to the existence of the market tempting trades of cyber sexual violence images, the illegal commodity. The businesspersons of telecommunication such as webhards, being the instrument for spread, have the responsibility to block illegal images, however the webhard cartel between uploader-webhard company-filtering company and private information deletion company is aggravating the damages[5].

Figure 1. Spread and recirculation of cyber sexual violence.

Thus, this thesis would propose a monitoring system rapidly retrieving and deleting crime images to prevent revictimization through re-circulation and spread of cyber sexual violence images. The thesis consists of followings. Chapter 2, Relevant Studies, looks into definition, types and features of Cyber Sexual Violence. Chapter 3 observes Multi-media Retrieval methods and suggests a webhard monitoring system. Chapter 4 draws a conclusion.

2. Related Research

2.1. Definition of cyber sexual violence

The term, Cyber Sexual Violence, is generally described as “Acts imposing senses of displeasure and threatening from personal information postings in relation to erotic message communication, sexual communication requests and sexual issues by means of undesired words or images which are not agreed by the other in cyberspace such as the Internet”[6].

Korean Response Center against Cyber Sexual Violence insists “the term includes not only online sexual harassment, online-based prostitution, manipulation/exploitation of sexual images, online/Internet-based sexual violence, digital sexual violence and gender-based violence causing sexual harassment on cyberspace, media and SNS by spreading, threatening, storing and posting body images of another via media such as camera without any agreement or consent, but also the spatial and technical meanings for behavioral mediation. This refers a need of enlarging the previous cyber space from the linkage between computers and virtual space
connected through the Internet to the linkages between digital devices including mobile phones and the virtual space”[7].

2.2. Sexual violence crime

The handbook for cyber sexual crime damages categorized the crime traits into 6 sections for descriptions[8]. First feature of cyber sexual violence is spatial characteristic. It is difficult to punish the assailant if the assailant or the business server is located overseas. Moreover, the victim may not acknowledge the damage or take long time to acknowledge, and even mentally suffer from the uncertainty, whether the person in the image/video is the person-self or not. Second feature, which derives from the assailants is, - due to many anonymous sympathizers, awareness and the sense of guilt to crime is low, age and social positions of assailants are not constant, accessibility to the crime images is high at all age groups through online media such as mobile phones, and high chances of dating abuse and sexual violence are anticipated if the assailant is the ex. Third feature derives from victims. As the victims of unconsent sexual images cannot assure whether they are filmed in the images and the images are distributed, psychological damages such as anxiety to further distribution follows. Furthermore, due to stalking and threats by assailants through crime images, difficulties in isolating assailants and victims, in finding who the assailants are and in social lives may be caused.

**Table 1.** Cyber sexual violence by behavioral types and sorts[8].

<table>
<thead>
<tr>
<th>Types</th>
<th>Features</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filming</td>
<td>-Install/direct filming -Filming against the will of the self or of others. High probability of further spread</td>
<td>-Illegal filming(so-called hidden camera) - (Part of body) upskirt, back, entire body, face and naked body - (Behavior) relieving oneself, sexual relations</td>
</tr>
<tr>
<td>Spread/ re-circulation</td>
<td>-Spread/Re-circulation of sexual relation images -Including images with the consent of the person(the person as the first distributor) -Regardless of the consent for filming and of the consent for distribution, spread/re-circulate via telecommunication networks -Spreading manipulated images or composite of face and sexual images</td>
<td>-Uploader(heavy uploader incl.) -Spread via group cat, SNS, porn websites, communities -Vindictive spread -Spreading via SNS accounts to insult acquaintances</td>
</tr>
<tr>
<td>Spread threatening</td>
<td>-Threats to spread images of sexual relations -Threats to spread sexual images to fulfill purposes such as harassment</td>
<td>-Threats to spread to family members and acquaintances -Threats for the hope of meeting again after breaking up -Conciliating not to spread the image if they meet again -Threats to spread the images for money</td>
</tr>
<tr>
<td>Distribution/ consumption</td>
<td>-Abetting and Cooperating spreads of cyber sexual violence images for profit -Consuming the sexual images without a consent via watching, sharing and saving them</td>
<td>-Platform licensee of webhards and porn websites -Platform users of webhards and porn websites -Re-spreaders aggravating the damage</td>
</tr>
<tr>
<td>Sexual harassments in cyberspace</td>
<td>-Behaviors of Defamation and Insults through sexual contents in cyberspace -Occurs in cyberspace such as SNS, text messages, e-mails, open communities, game chats and mobile websites</td>
<td>-Posting insulting sexual contents against the victim with the victim images -Posting undesired sexual images or videos(links) -Sexual harassments in cyberspace</td>
</tr>
</tbody>
</table>
Even if the victims request for supports to organizations for women and investigative agencies, active response is hardly expected due to the fear of image re-distribution and disclosure of personal information. If the scene of cyber sexual violence is accommodations or public places, anyone can be the victim on occasion, and there is an anxiety of not being recognized as victims of the sexual violence. Fourth, cyber sexual violence and its relevant crimes are highly related to actual sexual violence such as compensated dating, quasi-rape, stalking, house/public place breaking and dating abuse, and can be linked to illegal promotions to illegal drugs such as aphrodisiac, gambling and prostitutions. Fifth, professional techniques to delete cyber sexual violence images and collect relevant evidence are required. Lastly, as the cyber sexual crimes are connected to distribution and capital markets such as webhard companies, considering the social structures, punishment would not be sufficient mean to eliminate the crime, and as the information deleting companies, digital/cyber undertakers, are being more commercialized, financial and psychological damages to victims often occur. In addition, unlike sexual crimes such as rape or sexual molestation, the crimes are depicted through insignificant languages such as ‘hidden camera’ and ‘curiosity’, disclosure and accusation against the assailants from the dimension of social movement is difficult to be conducted due to the fear of re-distribution, and professional support facilities are insufficiently provided as the cyber sexual crime is personalized.

Crime images distributed online is spread rapidly through SNS, P2P sites, communities, illegal websites and webhards which ensures a complete anonymity. Once an image is distributed, the image is re-distributed consistently regardless of the persons directly involved, and the damage is aggravated. If anyone downloads the crime image and stores it into one’s hard-drive, the image is likely to be stuffed as potential crime image. Hence, cyber sexual violence present more severe and unrecoverable damage to victims compared to other sexual crime types[3][9].

3. Webhard Monitoring System

3.1. Retrieval methods

Image Retrievals incorporates the method to search the original. The techniques can be segmented to Text-Based Image Retrieval(TBIR), Content-Based Image Retrieval(CBIR), and Semantic-Based Image Retrieval(SBIR).

TBIR is a technique to manually comment on images, having users retrieving images to utilize queries to request all images appropriate to criteria based on the comments[10].TBIR is time-consuming as its large task amount, image comments, is manually performed. CBIR is often referred to Material-based Image Retrieval. Image features such as color, shape and texture are registered into Feature database, then appropriate images are retrieved based on the data stored in it[11].CBIR is performed via 2 phases – first phase is to extract image traits and store them into database. Second phase, a phase for online searching, is to retrieve any uploaded image on the Internet by using retrieval robots, compare the traits newly posed from the images and the ones stored, and then to transfers images with the highest level of similarity to users[12][13].

SBIR is a technique which integrated the TBIR and the CBIR – supplementing the existing drawbacks and improving retrieval accuracy[14].SBIR detects features of each objects and interest areas by using similarities in color, shape and texture. The detected fields and traits acquire semantic description of images stored in database through the SBIR. From the stage of queries for image retrieval, semantic features are extracted via semantic characteristic translators and the most adequate notion to describe separate and group area or object is selected via semantic mapping. This mapping procedure employs machine learning technique, and its result is output in Textual Word format after having Image Annotation processing[5].
3.2. Proposal monitoring system

Figure 2. Proposed webhard monitoring system.

The proposal webhard monitoring system prevents re-distribution of the crime image by retrieving and deleting the cyber sexual violence images and enables tracking the person who spread the image on a webhard.

The proposal monitoring system consists of three modules – Features extraction, Retrieval and Blocking. Each module functions as followings.

Image Feature Extraction Module extracts features of cyber sexual violence images and store them into database. The module extracts features from the reported image by victims, filtered illegal pornographic images and other reported sexual crime images in the past. The feature of the images in extraction includes text information(image title, file name, et al.), image hash value, and image DNA(color, shape, texture and sound). Traits of Retrieval Module is to utilize the stored data in Feature database and to perform image retrieval on webhards. Blocking Module examines similarities in retrieved images, download the image for identification, and send the result to webhards. The personal information of spreaders of crime images, original crime image, and the database storing cyber sexual crime images are managed by the module.

Once the victim of cyber sexual violence acknowledges the damage and report, following procedures are performed.

1. Features are extracted from the crime image reported by the victim.
2. Using the extracted feature, retrievals are performed on webhards.
3. Once any image with high similarity index with crime image is retrieved, downloading is performed.
4. Downloaded image is checked, and if the image is relevant, the result is reported to the webhards.
5. Webhards blocks any access to the crime image, check the personal information of the distributor. Moreover, all crime images existing on the webhards are to be deleted.

6. Webhards transfers entire processing result and personal information of the distributor to Blocking Module.

7. Blocking Module stores the data received from the webhards into cyber sexual crime database and utilize them.

4. Conclusion

As distributed cyber sexual crime images online are rapidly spread via SNS, communities, illegal websites and webhards and the image may be stuffed by a random person downloading it, hence the severity of cyber sexual crime is unimaginably huge. Moreover, any crime image filmed and distributed to harm victims socially and morally, the crime image even contains personal information of the victims, therefore the victims face a critical damage and their daily life cannot easily be sustained. Cyber sexual crime image should rapidly be deleted through reports by the police and Korea Communications Standards Commission yet has not been effective performed. Victims are charged at high financial cost to private cyber undertakers, however, immoral cybers undertakers, created cartel with webhards, re-distributed and often threatened the victims with the image.

Hence, this thesis proposes a monitoring system to rapidly and accurately monitor webhards. The proposal webhard monitoring system retrieves and deletes cyber sexual crime image to prevent re-distribution, and even allows tracking the first distributor of the crime image in the webhards. Considering the characteristics of cyber sexual violence — unavailability of victims to recognize their damage and time-consuming cost to recognize the damage — immediate blocking and deleting the cyber sexual violence image is urgently necessary regardless of the request by victims.

Cyber sexual violence images rapidly and easily being distributed on the Internet cause a constant suffering to the victims. The academia, government and private organizations should cooperate to find more systematic relief support measures for victims from cyber sexual violence.

5. References

5.1. Journal articles


5.2. Thesis degree


5.3. Books


5.4. Additional references


6. Contribution

6.1. Authors contribution

<table>
<thead>
<tr>
<th>Initial name</th>
<th>Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>LJY</td>
</tr>
<tr>
<td></td>
<td>-Set of concepts ✔</td>
</tr>
<tr>
<td></td>
<td>-Design ✔</td>
</tr>
<tr>
<td></td>
<td>-Getting results ✔</td>
</tr>
<tr>
<td></td>
<td>-Analysis ✔</td>
</tr>
<tr>
<td></td>
<td>-Make a significant contribution to collection ✔</td>
</tr>
<tr>
<td></td>
<td>-Final approval of the paper ✔</td>
</tr>
<tr>
<td></td>
<td>-Corresponding ✔</td>
</tr>
<tr>
<td></td>
<td>-Play a decisive role in modification ✔</td>
</tr>
<tr>
<td></td>
<td>-Significant contributions to concepts, designs, practices, analysis and interpretation of data ✔</td>
</tr>
<tr>
<td></td>
<td>-Participants in Drafting and Revising Papers ✔</td>
</tr>
<tr>
<td></td>
<td>-Someone who can explain all aspects of the paper ✔</td>
</tr>
</tbody>
</table>
6.2. Authors profile

<table>
<thead>
<tr>
<th>Author</th>
<th>Lee Jae-young / Semyung University Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.A.</td>
<td>Semyung University</td>
</tr>
<tr>
<td>M.A.</td>
<td>Semyung University</td>
</tr>
<tr>
<td>Ph.D.</td>
<td>Chungbuk National University</td>
</tr>
</tbody>
</table>

Research field

Major career
- 2012~present. Semyung University, Assistant Processor