March - April 2020
ISSN: 0193-4120 Page No. 4679 - 4687

Victimization of Women in Digital Era: Indian Legislative Approach

Asha Rawat [1], Preeti Sanger [2]

[1,2] Assistant Professor in Banasthali Vidyapith, India,

Article Info
Volume 83
Page Number: 4679 - 4687
Publication Issue:
March - April 2020

Article History
***Article Received**: 24 July 2019*
***Revised**: 12 September 2019*
***Accepted**: 15 February 2020*
***Publication**: 27 March 2020*

Abstract

Impulse noises in images are caused by bit errors in transmission and signal acquisition. Salt and pepper noise and random noise are also known as Impulse Noise. As per the statistical analysis of noise in Brain MRI image shows salt and pepper noise is one of the most common which affect the accuracy of the tumor detection. Many nonlinear algorithms have been proposed to remove salt and pepper noise. But without damaging the edges is the difficult Task. Noise removal without damaging the edges is proposed in this paper. If the noise density increases, the effectiveness of the filter will be decreased. This is the major drawback of the existing algorithms. This paper discusses many noise removal techniques and proposes a novel noise removal technique using Continuous Decision Based Multi Kernel Median Filter (CDBMKMF). The proposed CDBMKMF algorithm attempts to eliminate noise in high noise density images with better PSNR values. Image pixels are checked for the occurrence of salt and pepper noise and removed effectively. Using Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR), the proposed methods are validated and compared with existing algorithms. This paper also evaluates the proposed algorithm with standard and unsymmetrical median filters.

Keywords; *Noise Removal, CDBMKMF, unsymmetrical median filter, standard median filter*

I. INTRODUCTION

In present digitalization world every day starts with the technology and ends with the technology. Every class and person of at any age uses the technology. Everything in this world has two sides both negative and positive. As the technology develops its uses also develops some use it as tool for benefits and some use it as weapon for committing crime. In today's digital era, women and children were observed to be the major victims. Victimization of women is a global phenomenon they are considered a soft target by cyber criminals. For combating cyber crimes against women, the Information Technology Act 2000 was enacted on 9th June 2000. But this act is also not sufficient to cover the entire solution it has many lacunas and deficiencies. Modern world is witnessing enormous use of digital devices and is seeing the transformation from paper work to digital dependency. Being digitally literate has become the need of the hour. The growing need is creating such an impact on every person, resulting which Government of India has taken all possible initiatives to make India as Digital India. During the journey from real world to the virtual world, social Medias are getting flourished day by day. The reformation of digital world is somewhere lacking in proper and effective management in handling social sites. The volatility of digital world is also affecting the valuable time, energy, attention and resources of India.

II. CLASSIFICATION OF CYBER CRIMES AGAINST WOMEN

2.1 Cyber Stalking

Cyber Stalking is deemed to be the most common cyber crime committing over women and children

Published by: The Mattingley Publishing Co., Inc.

now days. The oxford dictionary defined as "pursuing stealthily". Cyber stalker regularly follows the movement of the targeted person on internet. There is no direct relation between cyber stalker and the person. Cyber Stalking usually committed against women and children because they are soft target. The main purpose behind is to harass or frighten a person. There are some essential of cyber stalking like posting of defamatory statements, always following and monitoring the online activity of person, sending of virus in order to destruct data, identity theft etc.

2.2 Cyber Spoofing

Cyber Spoofing means when someone or something pretends to be something else. The main aim of cyber spoofing is focused towards making effort for gaining someone's self-assurance, for getting unauthorized entree of system, to snip the information, snip the money, and towards spreading the malware. There are numerous methods of cyber spoofing like email spoofing, website or URL spoofing, caller ID spoofing, Text message spoofing and GPS spoofing, facial spoofing, extension spoofing.

In cyber spoofing men starts email mailing, send Whatsapp nude and vulgar photographs. They start praising the beauty of women and also start inquiry about the women and ask to have date with her.

2.3 Cyber Defamation

This is the publication of offensive statement or any material contrary to other individual through internet to derogate the reputation of the person. In cyber defamation, the sender sends email and other defamatory content with the objective towards defaming other individual. A huge harm and irreparable loss is caused against the victim. There are various medium by which cyber defamation could be executed like World Wide Web (WWW), discussion groups, Intranets, email lists and bulletin boards etc.[1]

Section 499, IPC defines defamation but in this definition no specific meaning is given regarding defamation on internet. There are various issues related to internet defamation.[2]

2.4 Sextortion

Sextortion is the act of extorting money or the sexual favours from someone by blackmailing or threatening to disclose or reveal evidences of person's sexual activity. It is type of virtual coercion to extort money and demand for sex. Now day's sextoration rise worldwide this is the practice of compelling the female to perform sexual act or threat to send her nude photographs. Anyone can be the victim of sextotation it can be a child or a women. In this type of crime cyber predator establish online relationship with the targeted women and stats flirting with her with romantic comments and appreciations and tries to gain the trust of women once he establish trust he starts threaten the female to send her sexually provocative pictures.

2.5 Cyber Bullying

Cyber Bullying means to harass, threaten, and discomfit another individual over the usage of Internet. Cyber bullying includes sending of photos, messages tweets, and post rude and aggressive text just for hurting or embarrassing another individual. Cyber bullying can be particularly damaging and upsetting because it is usually send by anonymous and it is hard to trace.[3]

2.6 Voyeurism

This deals with the act of tweeting in windows for watching unsuspicious individuals, typically women who were unclothing, naked, or who were involving in sexual acts. In these types of cases mostly the men are identified as voyeurs they get sexual pleasure by viewing the undressing or already nude women's. Mostly these criminals are mentally afflicted.

March - April 2020
ISSN: 0193-4120 Page No. 4679 - 4687

The main purpose of the criminal to have sexual pleasure and to click the photographs or to record the video.[4]

2.7 Harassment via e-mail

This act is considered to be a crime, where a women or another person can be harassed in cyber space. Also, this activity is observed to be a common phenomenon. Cyber harassment is same as the harassment through letters. Cyber Harassment shall take place in various forms via sexual, racial, and religious or in any other forms. This is therefore considered to be a serious violation of right of privacy of a person.

2.8 Pornography

Cyber Pornography can be called as dissemination of obscene material which includes sale distribution, promotion and exhibition of absence material through the medium of electronic mean. Pornography could be described as an explicit illustration of virtual sexual activities or descriptive activities for stimulating erotic other than aesthetic feelings, films, literatures etc.[5]

2.9 Morphing

Morphing is giving special effect or editing by using morphing tools available on internet to picture of a person. Usually females are victim of cyber morphing. Morphers[6] download the female's picture from their fake or real profiles from the social sites and then morph them to blackmail the females for fulfillment of their illegal demand of online sex chat.

2.10 Hacking

This is the practice of trying to take advantage or effectively taking advantage, or illegal entree to computer resources.[7]

In other view, Hacking is the violation of right of privacy and assault into the privacy of information via unlawful access. This was typically committed against women too by altering her entire profile into an obscene. There are various motives for cyber criminal to commit this crime like personal hatred feeling, to take revenge, just to time pass to have fun etc.

2.11 Trolling

This is another type of cyber crime against women in which conflicts occurs on internet and the criminal intentionally starts quarrelling and upsetting the victim by posting inflammatory messages in order to provoke the victims to get emotional response. Their main purpose is to create the cold war atmosphere in the cyber space.

III. CASE STUDY

A girl named Vinu Priya aged 21 years old from salem had completed her graduation in science stream. Accused has posted her nude morphed pictures on facebook. She passes through severe mental trauma. Investigation officer presumed that she was in relationship with the accused. she was being asked several questions she felt humiliated and at last she hanged herself[8]

Ritu Kohli case is the principal case of cyber stalking reported in India, where the cyber stalker used her candidature for chatting over internet. She also complained that stalker was giving her address online and using the absence language. She used to get the call in odd hours. Police investigated the matter and arrested the accused, and a case was filed based on section 509 Indian Penal Code 1860 for offending the modesty of women.[9]

In 2004, the DPS MMS case in which the obscene material was put up for sale on the site, Bazee.com and was widely circulated it was the clear violation of Section 67 of IT Act 2000.[10]

A doctor photographed and video recorded several women engaging in obscene activities that he distributed by internet in order to make illegal money and he was prosecuted under section 67 of IT Act, 2000.[11]

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4679 - 4687

A Swiss couple used to meet with slum youngsters and subsequently forced them for appearing in indecent photos. They used to upload them over few websites those were particularly intended for pedophiles. The Mumbai police had detained the accused over pornography, and were imprisoned towards this crime based on section 67 of IT Act read with 292 of IPC.[12]

In the July 2015 in Maharashtra the first conviction in cyber stalking case took place.[13] The Additional Chief Metropolitan Magistrate convicts the accused under Section 509 of IPC together with Section 66 E of IT Act 2008.

IV. CAUSES OF CYBER CRIME

- Digital illiteracy
- Globalization
- People don't want to read the term and condition of website they simply click the accept icon.
- Lack of awareness of cyber ethics.
- People don't care of uploading their profile picture sometimes also share their password.
- Lonely and neglected women like to participate in virtual socializing herself.
- Psychological weak women's.
- Posting of the emotional and depressing profile picture and status. It will attract the attention of cyber stalkers.
- Crises and emotional exploitation.
- Women are the soft target.
- Reason over passion towards love, to take vengeance and hatred, and for ego and power trips.
- Sometimes cyber crime is indebted for the sake of self recognition, fundamentally found in the youngster who always want to highlight in their group.
- To earn rapid money they are the greedy criminals they want to earn quickly by targeting the computer resource.

V. STATISTICS

The quantity of cyber crimes were found to rise exponentially in 2017 in contrast with that in 2016. Also it was noticed that, one in every five cyber crimes in 2017 was done beside a woman, as per the official data that was released in 2017 by National Crime Records Bureau (NCRB).

Around 21,796 cyber crime happenings were documented in 2017 in total, and a rise of 77% is seen when compared with 2016 figure of 12,317 as per the NCRB report of 2017. On the other hand, the 2016 figure was just 6% greater when compared to that of 2015 with a figure of 11,592.

Cyber Crime	Number
Cyber Blackmailing/Threatening	132
Cyber Pornography/Hosting/Publishing Obscene Sexual Materials	271
Cyber Stalking/Cyber Bullying of Women	555
Defamation/Morphing	50
Fake Profile	147
Other Crimes	3087
Total	4,242

Fig. 1. Source: The Indian Express Wednesday, December 18, 2019, NCRB Data: Cyber Crime jumped by 77% in 2017, written by Harikishan Sharma.

Over 50% of the happenings of cyber crime in 2017 have been driven by fraud, as per the report that was released on Monday. "During 2017, 56 per cent of cyber crime cases registered were for the motive of fraud (12,213 out of 21,796 cases) followed by sexual exploitation with 6.7 per cent (1,460 cases) and causing disrepute with 4.6 per cent (1,002 cases)."

Around 206 happenings of cyber crime have been recorded for provoking hatred against the country, and 139 have been observed to be done with political reasons. Around 110 cyber crimes have been recorded to be in relation with terrorist activities. Few women were not in a situation to report cyber crime grievance instantly.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4679 - 4687

VI. IMPACT OF CYBER CRIMES ON WOMEN

- Social and personal derogation
- End of personal life.
- Starting enjoying life in virtual world.
- Face continuous mental trauma.
- Ruin of Physical and mental health
- Enhance the tendency of suicide.
- Neglection of family.
- Females feel shy to report cases.

VII. INDIAN LEGISLATIVE APPROACH: CYBER LAW AND IPC

Chapter XI of the IT Act, 2000 corresponds with Cyber crimes wherein the actus reus is coupled with mens rea. It Act deal with the offences in which computer is used as either tool or target. In some offences the substantive law Indian penal Code 1860 applies along with IT Act, for example the offence of defamation through defamatory emails, reliance is placed on Section 500 of IPC 1860, (Earlier Section 66A of IT Act ,2000 pursuant to IT (Amendment) Act , 2008 expressly dealt with this crime).

Before the IT (Amendment)Act 2008 was passes any threatening emails ,or criminal intimidating messages were dealt with under Chapter XXII of IPC 1860, which were later dealt in Section 66A(b) of the IT Act 2000.In Shreya Singhal v.UOI the Supreme court struck down this segment as unconstitutional because of ambiguous language of the Section. Based on the provision of IT Act, 2000, and Indian Penal code 1860 cyber criminals are punished under following sections.

Section 66-A. Punishments for conveying violent messages via communication services[14]

Any individual who attempts to forward violent messages via computer resources or by any communication devices,

Whichever data that is totally violent or possessing threatening appeal; or

Whichever data that is known to be untrue, however to cause aggravation, troublesomeness, threat, hindrance, offense, grievance, criminal pressure, hostility, hate or ill-will obstinately by using such computer resources or a communication devices,

Whichever electronic mails that causes irritation, troublesomeness or in deceiving or in misleading the recipient regarding the origin of such messages,

Shall be punishable over a period that might range over three years with penalty.

Section 66-B. Punishments for deviously getting appropriated computer resources or communication devices[15]

Individuals who deceitfully accepts or holds stolen computer resource or communication devices expressively or partaking in reasons for believing the same as stolen computer resources or communication devices, are liable to punishment together with sentencing of both description over a period extending upto 3 years and with fine ranging around 1 lakh rupees or both together.

Section 66-C: Punishment for identity theft[16]

Individuals who is falsely or deceitfully making use of electronic signatures, passwords or other unique identification features that belong to other individuals, will be subjected to punishment with imprisonment for around 3 years and also presumed to be fined upto 1 lakh rupees for this case.

Section 66-D: Punishment for cheating by personation with the usage of computer resources[17]

Individuals who are attempting towards cheating by personation by any form of communication devices or computer resources, shall be liable to punishment with imprisonment for a period that may be extended to around 3 years and also shall be fined upto a sum of 1 lakh rupees for this particular activity.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4679 - 4687

Section 66-E. Punishment for violation of privacy.[18]

Individuals who are purposely or meaningfully violating the privacy shall fall prey under this section. He/she who distributes or spreads the photos concerning private area of any individual without their prior agreement, and in cases of violating the privacies of those individuals shall be subjected to punishment over a period ranging around 3 years together with imprisonment, and also shall be fined upto 2 lakh rupees for partaking in this activity.

Section 67. Punishment for Publishing/transmitting obscene materials in electronic forms[19]

Individuals who attempt to publish or transmit or cause towards punishment in any electronic forms, materials which are lascivious or appealing towards indecent interests or if its effects were towards tending to degrade and immoral person who is prospectively having regard to all pertinent situations, reading, seeing or hearing the matter confined or embodied in it, shall be subjective to punishment with imprisonment for a period of around 3 years and shall be fined upto 5 lakh rupees, and in cases of second attempt of such severe mistakes, imprisonment shall be extended upto 5 years along with the fine amount of 10 lakh rupees.

Section 67-A. Punishment for publishing/transmitting the materials encompassing sexually explicit contents in any electronic forms[20]

Individuals who are attempting to publish or transmit or being a cause of transmitting or publishing the materials that has sexually explicit contents via any electronic forms, shall be subjected to punishment in his/her first attempt with descriptive imprisonment that may range upto 5 years and shall be fined upto 10 lakh rupees, but if the person convicts the same for second attempt, he/she shall be made to take imprisonment that may extend upto 7 years along with fine amount of 10 lakh rupees.

Section 67-B Punishment for publishing/transmitting the materials that depicts children with sexually explicit contents in any electronic forms.

Individuals who:

(a) Publish or transmit or being a cause to publish/ transmit those materials in any electronic forms that depict children to be involved in any sexually explicit activities or conducts or,

(b) Create texts or digital image, collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing the materials in any electronic forms that depicts children with indecent or offensive or sexually explicit way, or

(c) Cultivate, entice or induce the children towards online relationships and on sexually explicit activities or in a way that might insult sensible adults on computer resources, or

(d) Facilitate abusing of children via online mode, or

(e) Records in any electronic forms in abusing or pertaining towards sexually explicit activities involving children, shall be subjective to get punished in the first attempt with the imprisonment that may be extending to 5 years and shall be viable to be fined upto 10 lakhs, and in the second attempt, the concerned individuals shall attain imprisonment that might be extending upto 7 years and shall be fined that might be extending to 10 lakh rupees.

Section 67/Section 67A and their provisions shall not be extended to any books, pamphlets, paper writings, drawings, paintings, representations or figures in any electronic forms-

(i) The publications that justifies them to be of public goodness in accordance that these books, pamphlets, paper writings, drawings, paintings, representations or figures falls under the coverage of

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4679 - 4687

sciences, literatures, arts or learning or other object of general concerns, or

(ii) Which were utilized to cover bonafide heritages or religious purposes: It should be noted that, in this section, "children" refers to individuals who have not crossed eighteen years of age.

Section 72. Punishment for breaching confidentiality/ privacy:[21]

Individuals who in pursuant of any of the powers deliberated under this Act, rule or regulation prepared there under, has secured accessing towards any electronic records, books, registers, correspondences, data, documents or other materials deprived of the agreement of the concerned individual reveals such electronic records, books, registers, correspondences, data, documents or other materials to any other individual shall be liable to punishment with imprisonment for a period extending upto 2 years and shall be fined upto 1 lakh rupees, or both punishments being given together.

Section 72-A. Punishment for disclosing information in breach of lawful contracts[22]

Any individual, containing an intermediate person who, while offering his/her service under the terms of legal agreement, has secured accessing towards any materials that contains personal data regarding another individual, with the intention in causing or knowing that he is probable in causing illegal losses or illegal gain discloses, deprived of the approval of the individual concerned, or in breach of a legal contracts, such materials to any other individual shall be liable to punishment with imprisonment that might extend upto 3 years, or shall be fined with a sum amount of upto 5 lakh rupees, or both punishments being provided together.

Section 77-A. Compounding of Offences.

A Court of experienced jurisdiction might compound offence other than offence for which the punishments for life imprisonments for a term beyond 3 years has been delivered under this Act. Provided additionally that, the Court will not compound any offences that affect the socio-economic condition of the nation or has been over children below eighteen years of age or over a woman.

Section 441 IPC. This section mainly concerns with the criminal trespassing activities.

Section 354D. This section mainly concerns with stalking. This sections describes ‘stalker’ as a male individual who keeps following a female individual and keeps trying to get in contact with her, who keeps monitoring all the activities done by her when she is using the digital media[23]

VIII. CHALLENGES

The criminal justice system in India has attained maturity over a period of more than a century and half and has earned international reputation as one of the efficient judicial systems of the world. The vital agencies concerned with administration of criminal justice include the parliament the law makers and the police law enforcers, the prosecutors, lawyers and the judges.[24] But if we talks about the cyber crimes Judiciary faced many challenges:

- Cyber crime cases are of Global nature and they do not recognize geographical or territorial boundaries.
- Ambiguity in exclusive Jurisdiction of court.
- Variation in the legal system and laws an procedure of different countries as regards admissibility of cyber crimes.
- Lack of proper investigation and lack of proper remedies.
- Improper enforcement of Cyber Laws.
- Long process to deal with cyber complaints due to lack of Cyber Forensics laboratories.
- Not enough numbers of e-courts.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4679 - 4687

IX. SUGGESTIONS AND RECOMMENDATIONS

- Organize digital awareness programme at large level.
- Introduction of IT course related to security and the cyber ethics from the school level.
- Establishment of Cyber Cell specifically for women's.
- Appointment of cyber Expert.
- Enforcement of present level and introduction of new stringent laws.
- Avoid disclosing personal information general awareness programme on e-safety and e-security.
- Strengthen the Indian education system.
- There are several reasons for committing cyber crime lie break up with your partner in this situation tries to change all online passwords or your details.
- After posting your photos online through social media always turn off the location services of metadata in the photo taken on mobile phone.
- Don't post online your private online calendars and your forthcoming events.
- Always log out from your PC after our work done.
- Don't response to message or bulletin board item which consists of obscene material.
- Don't meet with any stranger on the basis of online friendship.
- Always follow the privacy option.
- Harmonization of international legislations and encourage coordination and cooperation between national law enforcement agencies.

X. CONCLUSION

Crimes against women is not a current phenomenon, Women are from past facing crimes against them, as the times changes the way of committing crimes also changed. With the advent of technology the cyber crimes emerges and the people start committing crimes through electronic media and the women is the soft target. Through this paper researchers depicted various cyber crimes committed against women in today's digital era and also proposed some suggestion and recommendations like strengthen government policies, for appointment of a person in Police force he/she should possess cyber qualification and should be trained enough to deal with these types of cases. Social awareness programme etc. should also be conducted.

REFERENCES

[1]http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html

[2] See 2006 Cri LJ,Journal Section, at page 86.

[3]https://kidshealth.org/en/teens/cyberbullying.html

[4] https://www.sciencedirect.com/topics/medicine-and-dentistry/voyeurism

[5] Oxford English dictionary,2000.

[6] Morpher is a cyber criminal who illegally download the picture of a female from the social site and edit or morph them to blackmail women or her family by threatening to publish the morphed image to meet illegal demands of online sex chat.

[7] Section 66 of Information Technology Act 2000.

[8] Laws to Safeguard Women against Cyber Crimes in India
legaldesire.com. 20 May at 6:53 am.

[9] Cyber Crime In India: Are Women A Soft Target
By Deepshikha Sharma.

[10] "Bazee.com case-why I.P.C was not invoked?'' ,Business line,24th Dec,2004,available at:http://www.thehindubusinessline.in/2004/12/21/stories/2004122100110900.htm.

[11] M.Saravanan&Dr.L.Prakash v.state, Decided by the Hon'able High Court of Madras on 16th March,2006.

[12] State of Tamil Nadu V. Suhas katti ,decided by the Additional Chief Metroplitan Magistrate,Egmore on November 5,2004.

Published by: The Mattingley Publishing Co., Inc.

[13] Yogesh Prabhu v. State of Maharashtra, decided by theAdditional ChiefMetropolitan Magistrate M.R.Natu
[14] The Information Technology Act, 2000 (21 of 2000)
[15] Ibid.
[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Indian Penal Code ,1860 (Act No. 45 of 1860)
[24] Panday Ashish :Devition and prevention (2006)p.57