IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

A Empirical Study on Steganography in Tamilnadu

U. Varun Kumar[1] and Ms. Umamaheswari U[2]
BA. LLB (Hons)[1]
Assistant Professor[2]
Saveetha School of Law, Saveetha institute of Medical and Technical sciences (SIMATS), Chennai
uvarunkumar46@gmail.com and umamaheshwariu.ssl@saveetha.com

Abstract: *Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination. Content concealed through steganography is sometimes encrypted before being hidden within another file format. If it isn't encrypted, then it may be processed in some way to make it harder to detect. As a form of covert communication, steganography is sometimes compared to cryptography. However, the two are not the same since steganography does not involve scrambling data upon sending or using a key to decode it upon receipt. The term 'steganography' comes from the Greek words 'steganos' (which means hidden or covered) and 'graphein' (which means writing). Steganography has been practiced in various forms for thousands of years to keep communications private. For example, in ancient Greece, people would carve messages on wood and then use wax to conceal them. Romans used various forms of invisible inks, which could be deciphered when heat or light were applied. Steganography is relevant to cybersecurity because ransomware gangs and other threat actors often hide information when attacking a target. For example, they might hide data, conceal a malicious tool, or send instructions for command-and-control servers. They could place all this information within innocuous-seeming image, video, sound, or text files*

Keywords: hidden files, transparency, decoded, steganography

I. INTRODUCTION

Steganography works by concealing information in a way that avoids suspicion. One of the most prevalent techniques is called 'least significant bit' (LSB) steganography. This involves embedding the secret information in the least significant bits of a media file. For example: In an image file, each pixel is made up of three bytes of data corresponding to the colors red, green, and blue. Some image formats allocate an additional fourth byte to transparency, or 'alpha'. LSB steganography alters the last bit of each of those bytes to hide one bit of data. So, to hide one megabyte of data using this method, you would need an eight-megabyte image file. Modifying the last bit of the pixel value doesn't result in a visually perceptible change to the picture, which means that anyone viewing the original and the steganographically-modified images won't be able to tell the difference. The same method can be applied to other digital media, such as audio and video, where data is hidden in parts of the file that result in the least change to the audible or visual output. Another steganography technique is the use of word or letter substitution. This is where the sender of a secret message conceals the text by distributing it inside a much larger text, placing the words at specific intervals. While this substitution method is easy to use, it may also make the text look strange and out of place since the secret words might not fit logically within their target sentences. Other steganography methods include hiding an entire partition on a hard drive or embedding data in the header section of files and network packets. The effectiveness of these methods depends on how much data they can hide and how easy they are to detect. Steganography and cryptography share the same goal – which is to protect a message or information from third parties – but they use different mechanisms to achieve it. Cryptography changes the information to ciphertext which can only be understood

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, August 2025 Impact Factor: 7.67

with a decryption key. This means that if someone intercepted this encrypted message, they could easily see that some form of encryption has been applied. By contrast, steganography doesn't change the format of the information but instead conceals the existence of the message. Steganography works by concealing information in a way that avoids suspicion. One of the most prevalent techniques is called 'least significant bit' (LSB) steganography. This involves embedding the secret information in the least significant bits of a media file. For example: In an image file, each pixel is made up of three bytes of data corresponding to the colors red, green, and blue. Some image formats allocate an additional fourth byte to transparency, or 'alpha'. LSB steganography alters the last bit of each of those bytes to hide one bit of data. The main objective of this research is to negative impact of steganography in Tamilnadu.

OBJECTIVES :

- To study the nature of steganography.
- To examine the positive impact of steganography among public.
- To study the illegal activities caused through Steganography.
- To determine the legislatures for steganography.

II. REVIEW OF LITERATURE

Alex Norman (2011) Classical Steganography, This includes historical methods like hiding messages in wax tablets or invisible ink. While outdated, it laid the foundation for modern steganography. **Jessica fridrich (2010)**LSB Substitution, Least Significant Bit substitution is one of the simplest and widely-used techniques, where information is hidden in the least significant bits of image or audio data. **Abid yahya (2018)**Transform Domain Technique, These methods involve transforming the cover media into a different domain (e.g., frequency or wavelet) before embedding data. Techniques like Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) are common. **Peter wayner (2002)** JPEG Steganography, Focused on hiding data within JPEG images without significantly degrading image quality. Methods often manipulate the quantization tables or coefficients. **Gregory kipper (2003)** Audio Steganography: This branch conceals data within audio files. Phase coding and spread spectrum are among the techniques used. **Chun shien (2004)**Video Steganography: Like audio, video files can also be used to hide data. Temporal and spatial domain approaches are employed here. **Gandharba (2019)** Steganalysis: The study of techniques to detect hidden information. It's an ongoing cat-and-mouse game with steganographers, where researchers develop methods to reveal hidden data. **Audrey coon (2015)** Information Theoretic Approaches: Research into the theoretical limits of steganography, often involving measures like the Rate-Distortion function. Machine Learning in Steganography: More recently, the integration of AI and machine learning techniques for both steganography and steganalysis has gained attention. **Mahmound hassaballah(2020)**Steganography: As the digital world evolved, steganography has expanded to cover various multimedia types, including text, images, audio, and video.Security Applications, **Neilf. Johnson(2013)**Beyond covert communication, steganography is also applied in digital watermarking and copyright protection. by various factors. Detection Challenges, One of the primary disadvantages is that steganography can be difficult to detect. **Zoran duric 2012)**This poses a risk in security-sensitive contexts, as malicious actors may use it for nefarious purposes. Data Loss, Embedding hidden data can lead to some loss of data fidelity, especially in media files like images and audio. **Sushil jajodia(2012)**This can affect the quality of the cover medium. Size Limitations: The amount of data that can be hidden within a cover medium is limited by its capacity. This restricts the volume of information that can be transmitted covertly. Security Risks, If not implemented correctly, steganography can introduce security risks. **Jagadish Chandra(2018)**Poorly designed systems may be vulnerable to attacks that reveal hidden data. Legal and Ethical Issues, The use of steganography can raise legal and ethical concerns, especially in cases involving privacy invasion, copyright infringement, or cybercrime. Complexity, Implementing steganography techniques can be complex, requiring specialized software and expertise. This complexity may deter some users. **Hitesh kumar (2019)**Risk of Misuse, While steganography has legitimate applications, it can also be misused for illegal or malicious purposes, such as concealing malware or conducting covert espionage. Detection: The primary problem with steganography is the difficulty of detecting hidden data. **Praveen kumar(2008)**This poses a significant challenge for law enforcement and security agencies when trying to identify covert communication. False

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, August 2025 Impact Factor: 7.67

Positives: Detection methods can generate false positives, leading to innocent data being flagged as suspicious. This can waste resources and cause privacy concerns. **Frank y.shih(2017)**False Negatives: On the flip side, false negatives can occur when steganography techniques are used effectively, and the hidden data goes undetected. **Arson sorout(2014)**Capacity Limitations: The amount of data that can be hidden within a cover medium is limited by its capacity. This limitation can be a problem when trying to transmit large volumes of data covertly. **Tomar kuldeep(2009)**Data Loss: Embedding hidden data can result in a loss of quality or fidelity in the cover medium, particularly in media files like images and audio.Key Management: Some steganography methods require keys or passwords for embedding and extracting data. Managing and securing these keys can be challenging, and their loss can lead to data inaccessibility. **Neha sawal(2013)**Ethical Dilemmas: The use of steganography raises ethical concerns, especially when it is employed for illegal or malicious purposes, such as concealing malware or conducting covert surveillance.Legal Issues: Depending on the jurisdiction, the use of steganography for certain purposes may be illegal, leading to legal consequences for individuals or organizations. **Peter wayner (2019)**Complexity: Implementing steganography techniques can be complex, requiring specialized knowledge and tools. This complexity can deter legitimate users and limit adoption. Misuse: Steganography can be misused for nefarious purposes, including cyberattacks, espionage, or facilitating criminal activities. This poses a security risk to individuals and organizations. **Ajith abraham(2015)**Continual Evolution: As steganalysis techniques improve, steganographers are compelled to develop more sophisticated methods, leading to an ongoing cat-and-mouse game in the field. Privacy Concerns: In some cases, steganography may infringe on privacy rights when used to conceal personal or sensitive information without consent.

III. METHODOLOGY

The researcher has adopted empirical research methodology for the purpose of doing this research. As the researcher not only collected sources of primary data but also collected secondary data. Primary Data was collected by administering a well-structured and non-disguised schedule, comprising 2 questions from people of tamilnadu by conducting surveys using random. Sampling Methods and Responses which researchers got from the people are about 200 responses. To analyze the graphical representation is used.sample method is Random sampling method was used for the purpose of this study.sample size is There are a total of 200 samples collected with regard to this study. independent variables are age, gender, occupation, educational qualification. The present paper was analysed through the non-doctrinal research methodology and empirical and descriptive method of research was used. The present analysis was made through a random sampling method where the survey was taken from common public, professionals, etc. The sample size in the present analysis is 200 samples, the independent variables in this analysis are age, gender, occupation and educational qualification. The research tools used in the present paper such as graphical representation was also used to analyze the study.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

IV. ANALYSIS AND INTERPRETATIONS

FIGURE 1

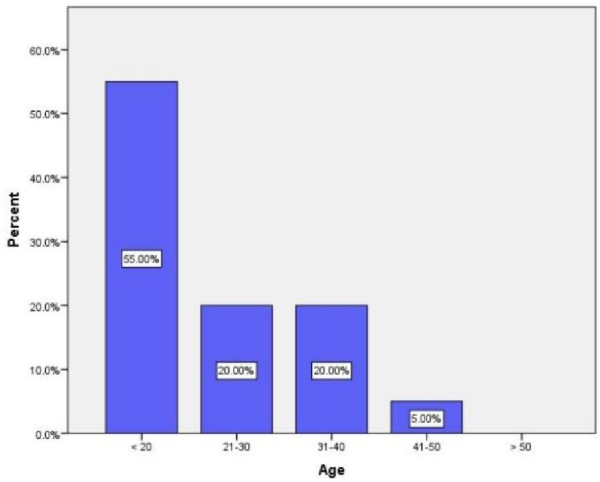
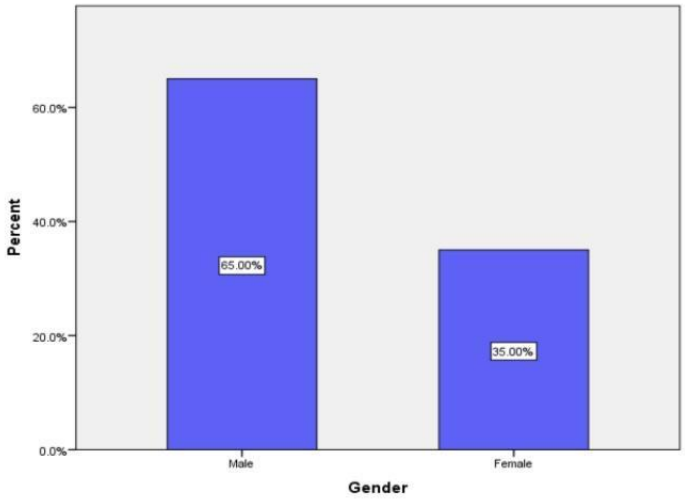


FIGURE 2



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

FIGURE 3

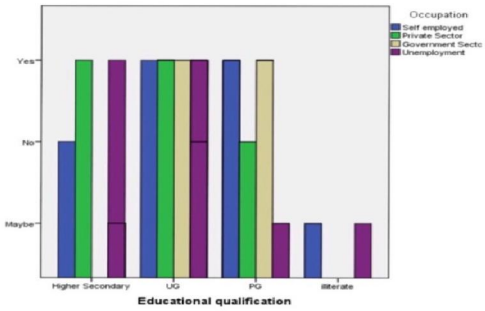
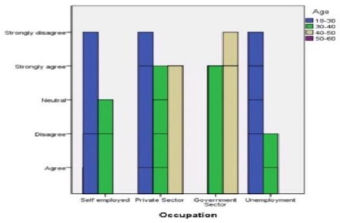


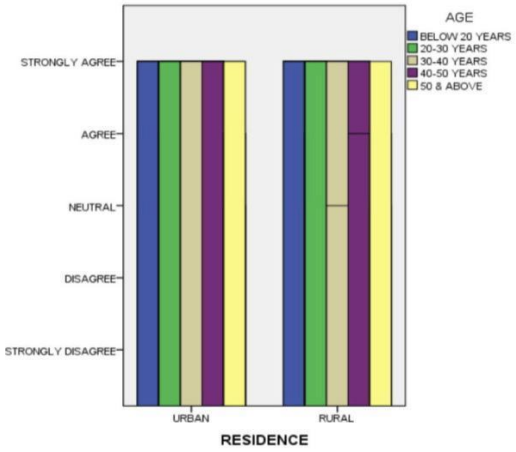
FIGURE 4



DOI: 10.48175/IJARSCT-28708

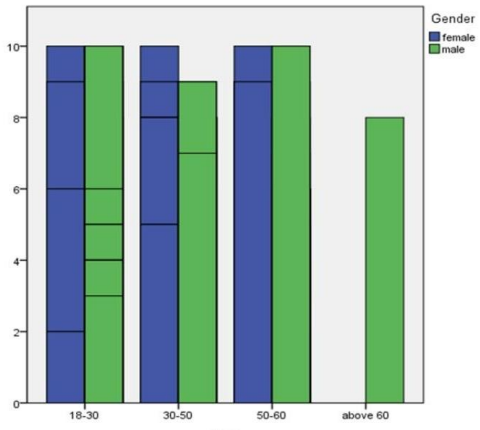
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

FIGURE 5



LEGEND : In the figure 5 represents the relationship between the question steganography is a technique of hiding information within other forms of digital media and this survey says that the people from urban are strongly agree to the statement.

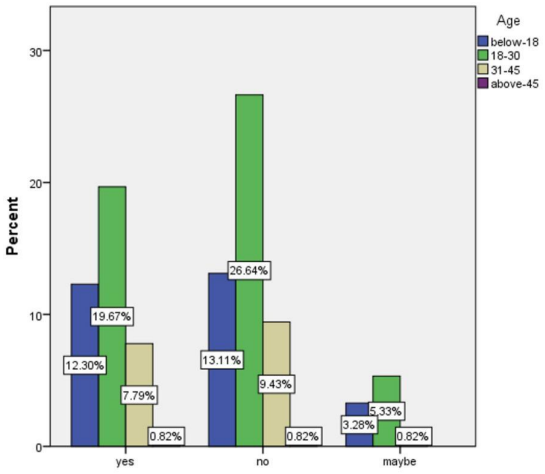
FIGURE 6



LEGEND : In the figure 6 represents the relationship between the question cyber criminals expolits to hide malicious code or communication within seemingly harmless file.

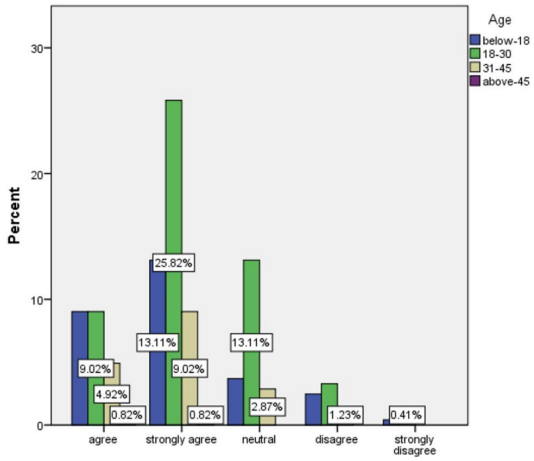
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

FIGURE 7



LEGEND : In this figure 7 represents the relationship between the question steganography can be used by various individuals or groups for different purposes.

FIGURE 8



LEGEND : In this figure 8 represents the relationship between the question encrypted keys are not a common medium used in steganography.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

V. RESULTS

The question was asked regarding whether they were aware of the term Environmental crimes and the dependent variable was occupation and the independent variable was educational qualification . People of the age group 18-30 mostly gave a combined answer of yes and no. People from the age group 30-40 mostly agreed while some of the respondents said no. People from the age group 40-50 answered yes. In (**fig 2)** The question steganography is a technique of hiding information within other forms of digital media . The (**figure 2)** represents the opinion of the respondents regarding whether they were aware of the term steganography evolved over the years and what are its key featureswas occupation and the independent variable was gender. Most of the males answered yes for the question asked with some of the respondents answered no. The female respondents gave a combined answer of yes and no. The (**figure 3)** represents the opinion of the respondents regarding steganography can be used by various individuals or groups of different purposes was occupation and the independent variable was educational qualification . For the question asked most of the higher secondary respondents mostly answered yes while some answered maybe. The Undergraduates and Postgraduates mostly answered yes where the illiterates respondents mostly answered no. The (**figure 4**) represents the opinion of the respondents regarding cyber criminals exploits steganography to hide malicious cod or communication within seemingly harmless file and the dependent variable was gender and the independent variable was occupation. Majority of the self employed respondents answered yes to the question proposed. Private sector respondents answered no mostly. Government employees and unemployed respondents mostly answered no.

VI. DISCUSSION

From the survey it is found that with the help of comparing the athe legal regulations and guidelines governing spiritual tourism in India nd comparing it with the gender of the respondents , most of the respondents in every gender agreed with the statement as they were well aware that rain is the vital source for human life **(Figure 1).** From the survey it is found that with the help of comparing the question whether they were aware of the term steganography and the criminals who exploits it and comparing it with the occupation of the respondents , most of the respondents in every kind of occupation agreed with the statement as they thought it was nearly impossible to survive without rainfall and its benefits on the planet earth.**(Figure 2).** From the survey it is found that with the help of comparing the question whether they were aware of the term steganography and its crimes and comparing it with the educational qualification of the respondents , most of the respondents agreed with the statement as they thought it was nearly impossible to survive without rainfall **(Figure 3).** From the survey it is found that with the help of comparing the question whether they were aware of the term Steganography can be used by various individuals or groups for different purpose crimes and comparing it with the gender and occupation as the dependent and independent variables of the respondents , most of the respondents agreed with the statement as they thought advantages are way more with than without rainfall.**(Figure 4).**Steganography is a technique used for hiding information within other forms of digital media. The (**figure 4))** represents the opinion of the respondents regarding whether they were aware that the term steganography is a technique used for hiding information within other forms of digital media. was occupation and the independent variable was gender. Most of the males answered yes for the question asked with some of the respondents answered no. The female respondents gave a combined answer of yes and no. The (**figure 5)** represents the opinion of the respondents regarding cyber criminals exploits steganography to hide malicious code or communication within seemingly harmless file was occupation and the independent variable was educational qualification . For the question asked most of the higher secondary respondents mostly answered yes while some answered maybe. The Undergraduates and Postgraduates mostly answered yes where the illiterates respondents mostly answered no. The (**figure 6**) represents the opinion of the respondents regarding encrypted key was not a common cover medium used in steganography and the dependent variable was gender and the independent variable was occupation.

VII. LIMITATION

The major limitation of the study is the sample frame. The restrictive area of sample size is yet another drawback of the research. Collection of data via online platform is limiting the researcher to collect data from the field. Since the data is

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

collected online platform wherein the respondent is not known,the original opinion of the respondent is not found. The researcher could only come to an approximate conclusion of what the respondent is feeling to convey.

VIII. SUGGESTIONS

Advanced Algorithms Develop and use more sophisticated steganographic algorithms that provide better security and make it harder for adversaries to detect hidden information.Encryption Integration: Combine steganography with encryption techniques to double-layer security, ensuring that even if the hidden information is discovered, it remains encrypted and unreadable.Multimedia Formats Explore steganography in emerging multimedia formats, such as virtual reality environments or 3D models, to expand the scope beyond traditional text and images.Machine Learning Defense: Anticipate advancements in steganalysis (the detection of steganographic content) by incorporating machine learning and artificial intelligence techniques into steganography to stay ahead of detection methods.Adaptive Embedding Develop steganographic methods that can adaptively adjust the amount of hidden data based on the host media, making it more resistant to detection.

IX. CONCLUSION

In conclusion, steganography is a multifaceted field with both advantages and disadvantages. It offers a means of covert communication, data security, and data integrity, making it valuable for various applications, including digital watermarking and authentication. However, it comes with significant challenges.The primary challenge lies in the difficulty of detecting hidden data, which poses risks in security-sensitive contexts. False positives and false negatives can further complicate detection efforts. Capacity limitations and potential data loss in the cover medium can affect the volume and quality of hidden information.Steganography also raises ethical and legal concerns, especially when misused for illegal purposes. Managing keys and dealing with the complexity of steganographic techniques can be problematic.Despite these challenges, steganography remains a powerful tool when used responsibly and ethically. Its effectiveness and appropriateness depend on the specific use case and the implementation of the technique. As technology continues to advance, both steganography and steganalysis will likely evolve, emphasizing the need for ongoing research and vigilance in addressing its implications for privacy, security, and communication.

REFERENCES

[1]. Sophie Namy, Andrea Norcini Pala, Milton L. Wainberg, Lori Michau, Janet Nakuti, Louise Knight, et al. 2020. "Violence against Children and Intimate Partner Violence against Women: Overlap and Common Contributing Factors among Caregiver-Adolescent Dyads." BMC Public Health 20 (1): 1–13.

[2]. Dr Lakshmi Vijayakumar and Dr Sukriti Chauhan. 2020. "When Children Get Caught between Domestic Violence, Online Abuse." Times Of India. May 28, 2020. https://timesofindia.indiatimes.com/india/when-children-get-caught-between-domestic-violence-online-abuse/articleshow/76064654.cms.

[3]. McGaha-Garnett, Valerie. 2013. "The Effects of Violence on Academic Progress and Classroom Behavior : From a Parent ' S Perspective." https://www.semanticscholar.org/paper/The-Effects-of-Violence-on-Academic-Progress-and-%3A-McGaha-Garnett/5fcec42a76544e1a5f5cbf749c5c94df4ef4be54.

[4]. "[No Title]." n.d. Accessed March 9, 2021. http://icancl.org/pdf/child-neglect.pdf.

[5]. Ortiz-Ospina, Esteban, and Max Roser. 2017. "Violence against Children and Children's Rights." Our World in Data, October. https://ourworldindata.org/violence-against-rights-for-children.

[6]. Pingley, Terra. 2017. "The Impact of Witnessing Domestic Violence on Children: A Systematic Review." St. Catherine University. https://sophia.stkate.edu/msw_papers/776.

[7]. "Realizing Children's Rights in India - Humanium." n.d. Accessed March 9, 2021. https://www.humanium.org/en/india/.

[8]. "Special Representative of the Secretary-General on Violence against Children." n.d. Accessed March 9, 2021.https://www.end-violence.org/members/special-representative-secretary-general-violence-against-children.

[9]. "Studies in Child Health: Research to Improve Health Services for Mothers and ." n.d. Accessed March 9,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

2021. https://books.google.com/books/about/Studies_in_Child_Health.html?id=AbDLXPUEaeIC.

[10]. Thoresen, S., M. Myhre, T. Wentzel-Larsen, H. F. Aakvaag, and O. K. Hjemdal. 2015. "Violence against Children, Later Victimisation, and Mental Health: A Cross-Sectional Study of the General Norwegian Population." European Journal of Psychotraumatology 6 (January). https://doi.org/10.3402/ejpt.v6.26259.

[11]. UNICEF. Executive Board (2008, annual sess. : New York). 2008. "The UNICEF Child Protection Strategy in Support of the Medium-Term Strategic Plan," June. http://digitallibrary.un.org/record/630690.

[12]. "Website."n.d.AccessedMarch9,2021a.https://www.researchgate.net/publication/279496860_Childhood_Experiences_of_Physical_Emotional_and_Sexual_Abuse_among_College_Students_in_South_India.

[13]. AccessedMarch9,2021b.http://www.journaldmims.com/article.asp?issn=0974-3901;year=2017;volume=12;issue=4;spage=253;epage=260;aulast=Tendolkar.

[14]. AccessedMarch9,2021c.https://www.jiaps.com/article.asp?issn=0971-9261;year=2007;volume=12;issue=2;spage=63;epage=64;aulast=Gupta.

[15]. https://www.ijcm.org.in/article.asp?issn=0970-0218;year=2019;volume=44;issue=4;spage=362;epage=367;aulast=Ram;type=0.

[16]. 2021e.https://www.indianjpsychiatry.org/article.asp?issn=0019-5545;year=2018;volume=60;issue=4;spage=494;epage=498;aulast=Patra;type=0.

[17]. https://www.jstor.org/stable/29515733.

[18]. https://www.researchgate.net/publication/51041975_Prevalence_of_Violence_against_Children_in_Families_in_Tripura_and_Its_Relationship_with_Socio-economic_Factors.

[19]. https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(17)30103-1/fulltext.

[20]. Human Rights Watch. 2019. World Report 2019: Events of 2018. Seven Stories Press.