

Privacy-Preserving Framework for Facial Reusage Recognition with Fingerprinting and Digital Image Protection in Law Enforcement

**Priti Das, Indranil Paul, Ananya Roy, Subha Karmakar,
Rohitashwa Pal Das, Somsubhra Gupta**

Department of Computer Science and Engineering,
Swami Vivekananda University, West Bengal -700121

Corresponding Author email IDs: ruhi929jk@gmail.com /
indranil.paul04@gmail.com

Abstract

This paper presents a framework that safeguards privacy while recognizing reused facial images, incorporating fingerprinting, and protecting digital images for law enforcement purposes.

The broad consumption of social media has contributed to the issues of protecting user privacy, notably illicit face picture reuse and data leakage. This study presents a revolutionary Digital Object Source Identifier (DOSI) system designed to identify the source of digital data breaches and provide strong security against unlawful replication and dissemination of visual material. DOSI uses cutting-edge approaches to secure traceability and ownership integrity for digital files, drawing analogies with copyright-claiming systems and advanced multimedia recognition technologies such as song identification by humming or tune analysis.

The system generates unique picture IDs using face recognition algorithms and digital fingerprinting techniques such as hashing. These identifiers assist in detecting and tracking repeated or derivative material across platforms. It also incorporates deep learning architectures, particularly Convolutional Neural Networks (CNNs), to accurately extract features and detect changed photos. Furthermore,

watermarking approaches integrate cryptographic ownership details into image pixels, improving tamper-resistance and traceability.

The solution system uses fingerprinting technology to monitor picture ownership, provenance, and usage history, assuring data integrity and preventing manipulation. It also makes use of web crawling and scraping techniques, as well as APIs like Google Reverse Image Search, to track illicit image distribution on social media and marketplaces on a broad scale. The DOSI system identifies data leaks and prevents abuse, providing critical support for law enforcement, digital content providers, and privacy-conscious consumers seeking better data security and accountability in an interconnected digital world.

Keywords: *Digital Object Source Identifier, Image Fingerprinting, Derivative Content Detection, AI-powered Facial Recognition*

I .Introduction

In this digital age, Social media is an integral part of our daily life whether it comes to technology, news, daily life, and whatnot. As a result, users need to upload images and videos to the platform. But the problem arises when users can't find enough privacy while sharing the image, and information in the vast world of social media. Data privacy and security have become paramount concerns for individuals and organizations alike. With the proliferation of online services, social media platforms, and interconnected devices, vast amounts of personal and sensitive data are being generated, stored, and transmitted across the internet. This data, while offering tremendous opportunities for innovation and convenience, also presents significant risks when misused or inadequately protected.

One of the major challenges in maintaining data privacy is the prevention of misuse by unauthorized entities, whether they be malicious actors, negligent insiders, or overly curious data handlers. The consequences of data misuse can be far-reaching, including identity theft, financial fraud, loss of confidentiality, and erosion of public trust. As such, there is a pressing need for robust frameworks that not only secure data but also ensure that it is used appropriately and ethically.

This research paper proposes a privacy-preserving framework designed to prevent the misuse of images and videos. The framework leverages advanced cryptographic techniques, access control mechanisms, and machine learning algorithms to detect and mitigate potential misuse scenarios. By implementing a multi-layered approach, the proposed solution aims to provide comprehensive protection for data while preserving user privacy and complying with relevant legal and regulatory requirements.

A) Social Media and User Safety

social media has emerged as a powerful tool for communication, interaction, and information dissemination. Social media platforms, such as Facebook, Twitter, Instagram, LinkedIn, and TikTok, have revolutionized the way individuals and organizations connect and share content. These platforms enable users to create and share text updates, images, videos, and other multimedia content, fostering a dynamic and interconnected global community.

Despite the numerous benefits offered by social media, there are inherent risks and concerns associated with sharing personal content, particularly images, online. The question of whether it is safe to upload images on social media has become a critical issue, encompassing various aspects of privacy, security, and digital footprint management. Users must navigate complex privacy settings, understand the implications of metadata associated with images, and be aware of the potential for misuse of their visual content.

This research paper aims to explore the multifaceted nature of social media and assess the safety considerations related to uploading images. This study seeks to provide a comprehensive understanding of the current landscape. Furthermore, it aims to offer practical guidelines and best practices for users to protect their privacy and ensure safe sharing of images on social media.

In recent years, the use of social media has increased gradually and the posting of multimedia has increased but the privacy user is not secured. Recent studies have highlighted the alarming issue of illegal harassment through the misuse of images without the owners' permission on social media.

A comprehensive review by MediaWell Research Review discusses how image-based abuse involves the non-consensual creation and distribution of personal images. This form of abuse has severe psychological impacts on victims, including severe emotional distress and even leading to self-harm in extreme cases. A study published in the journal Information & Communications Technology Law explores the complex nature of non-consensual image-based harassment worldwide. It highlights the legal challenges and the need for stronger policies to address this issue effectively.

According to records there are a large number of illegal face/ image misuse cases from social media per year worldwide, as many incidents go unreported or undetected and after spreading in all platforms (“VIRAL”), its was almost impossible to find out the main source and remove the image/ video from the root source.

For the solution of this alarming problem, this system will help to track repeated or derivative material across platforms.

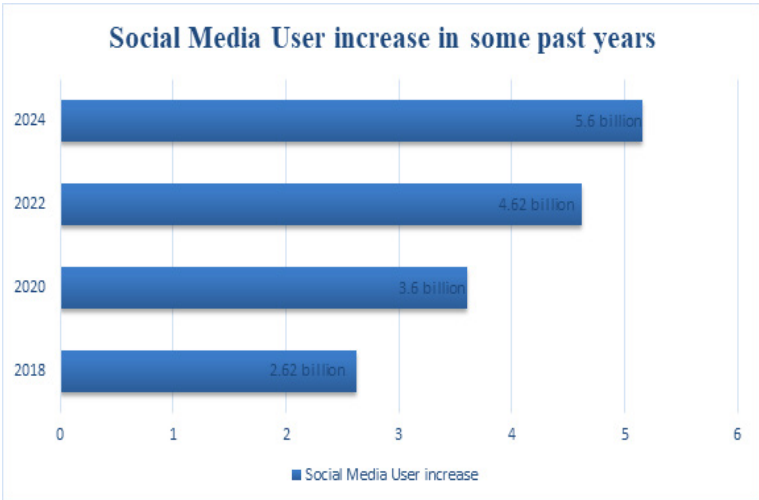


Fig 1: Social Media Users increase in some past years

B) Cyberbullying and Reports

Cyberbullying is a form of bullying that occurs on social media platforms mostly Instagram, Facebook, Snapchat, and other

media. Kids of, every age become victims of cyberbullying and the risk is increasing day by day with the increase of users. Cyberbullying includes sending, posting, or sharing negative, harmful contents about someone else illegally. And situation goes out of hand when the victim can not find the bully because the content goes viral. According to reports at least one-third of middle and high class students report for being a cyber bullying victim .After surveying since 2002 ,over 25000 students have been reported as being victim of cyberbullying. In a report of Cyberbullying Research Center that 27 percent of teens have been cyberbullied every year . In a survey of Cyberbullying Research Center ,over 5000 teenagers among them 25% students are being cyberbullied within a month .Every year in this survey since 2016 , the victims of cyberbullying is increasing rapidly .

According to cyberbullying researches ,parents of kids between the age of 10 to 18 , claimed about their children have been cyberbullied. 56% reports occurred during the mid of 2020 .And the cases increased during and after COVID 19 lockdowns.

According to January 2021 survey , 41% of internet users had experienced any kind of online harassment and among them 27% of reported about severe forms of online harassments.

Cyber bullying can take many forms causing life threatening situations ,as the bully can do anything with the posted images in the social media and then circulate it in another or same social media platform . Most of the social media companies are taking cyberbullying seriously now but the only option is to report the post to ban the specific account but its not the solution if the content goes viral with various accounts.

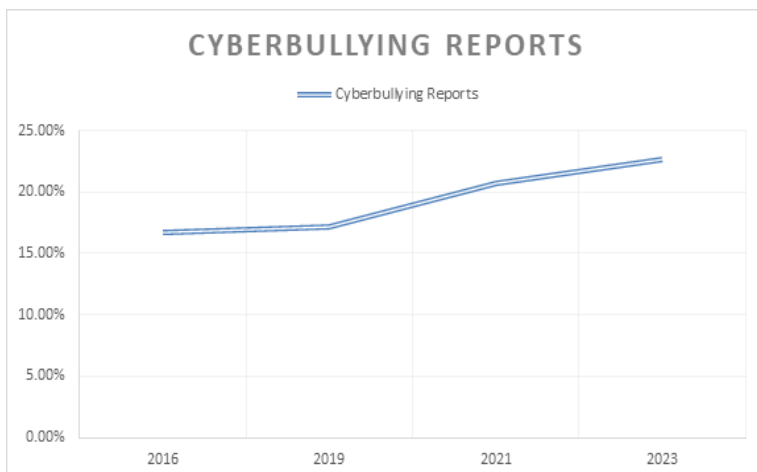


Fig 2 : Cyberbullying reports in some past years

Here comes the **Privacy-Preserving Framework for Facial Reusage Recognition with Fingerprinting and Digital Image Protection** system which can change the graph of cyberbullying by tracking the root sources of the bullying contents

II. Predictive Analytics

Predictive Analysis for Privacy-Preserving Framework in Facial Reusage Recognition for Law Enforcement.

The integration of a privacy-preserving framework for facial reusage recognition is poised to revolutionize the operational strategies and ethical standards in law enforcement and digital forensics. The proposed framework aims to address the critical challenges associated with privacy violations, data misuse, and security breaches in biometric systems by implementing cutting-edge techniques, including cryptographic algorithms, digital fingerprinting, and robust image protection. This predictive analysis outlines the potential impact and benefits of such a framework across various dimensions:

A) Enhancing Scalability and Interoperability

- The framework's modular architecture is expected to support seamless integration with existing law enforcement databases and tools.

- By adopting interoperable standards, the system will allow agencies to collaborate across jurisdictions without compromising privacy.

B) Reducing False Positives and Negatives

- Advanced fingerprinting and recognition algorithms will improve the accuracy of facial recognition systems, minimizing errors that could lead to wrongful identification or missed matches.

- Predictive models and AI-driven anomaly detection will enable real-time identification of potential misuse or manipulation of facial data.

C) Enabling Secure Cross-Agency Data Sharing

- Homomorphic encryption and secure multi-party computation will facilitate data sharing between law enforcement agencies while preserving the confidentiality of sensitive information.

- This secure collaboration will empower global efforts to combat cybercrime, trafficking, and terrorism.

D) Promoting Ethical AI Practices

- The framework will ensure fairness and bias mitigation in facial recognition systems, preventing discriminatory practices.

- Auditable mechanisms and explainable AI models will provide transparency in decision-making, ensuring accountability.

E) Adopting Blockchain for Data Integrity

- Blockchain technology can be integrated to create an immutable ledger for tracking the provenance and usage history of facial data.

- This will prevent unauthorized alterations and establish a robust chain of custody in forensic investigations.

F) Preparing for Post-Quantum Security

- The framework will incorporate quantum-resistant cryptographic techniques to future-proof the system against emerging threats from quantum computing.
- By anticipating advancements in computational power, it ensures long-term data security.

G) Empowering Victim Protection

- The system will allow individuals to report unauthorized reuse of their facial data, triggering secure takedown mechanisms and forensic tracing.
- Victim support services can leverage this technology to identify and mitigate digital exploitation cases effectively.

H) Streamlining Judicial Processes

- By providing tamper-proof evidence and detailed logs, the framework can expedite legal proceedings and improve the admissibility of digital evidence.
- Automated compliance checks with legal and regulatory frameworks will further ensure the admissibility of evidence in court.

I) Driving Innovation in Privacy-Centric AI

- The research is likely to inspire advancements in AI models optimized for secure computation, including federated learning and edge AI systems.
- These innovations will broaden the applicability of the framework across domains beyond law enforcement, such as healthcare and border security.

J) Fostering Public-Private Partnerships

- Collaboration between government entities, private technology firms, and academic institutions will be crucial for the development and deployment of the framework.
- Such partnerships will promote knowledge sharing, resource optimization, and faster adoption of privacy-preserving technologies.

K) Supporting International Compliance

- The framework will align with global data protection standards, such as GDPR, HIPAA, and ISO/IEC 27701, enabling cross-border implementation.
- Its compliance-ready design will make it a benchmark for other industries dealing with sensitive biometric data.

L) Contributing to Cybersecurity Workforce Development

- The deployment of this framework will necessitate training law enforcement personnel in advanced cryptographic and forensic techniques, fostering a skilled cybersecurity workforce.

In conclusion, the predictive impact of the privacy-preserving framework lies not only in enhancing the operational capabilities of law enforcement agencies but also in setting a new precedent for ethical, secure, and privacy-centric technologies. This transformative approach will ensure that advancements in biometric recognition align with societal values, legal norms, and technological foresight, making it a cornerstone in the future of secure digital law enforcement.

III. Methodology

Methodology refers to the systematic approach and procedures used to conduct research within the network. It encompasses the strategies, tools, techniques, and processes that guide how research is designed, carried out, analyzed, and evaluated across the collaborative network. This information allows readers to check whether the approach is accurate and dependable. A good methodology can help increase the reader's trust in their findings.

The system provides all the below stated functions and many more functions–

- Before posting an image in social media, face recognizer software recognizes all the faces in the image automatically,
- Generate Unique Hash ID (A-Hash, P-Hash, D-Hash etc.) for each faces in the image for Unique Fingerprinting,

- Invisible Watermarking and Invisible Fragile Watermarks are embedded to those facial images for special Identification,
- Once posted, Hash ID and watermarks and content ID will be stored in database,
- CNN (Convolutional Neural Networks) stores all the shares of the post in the form of Table.

When someone claims about the post, then the social media servers can trace the root source of the content(post) and wherever the content circulated by following process-

- AI detects the facial features , watermarks from the image,
- Matches the result with the database,
- If the unique ID matches, then it provides the source of the post
- Through CNN, all the shares of the post is accessible.

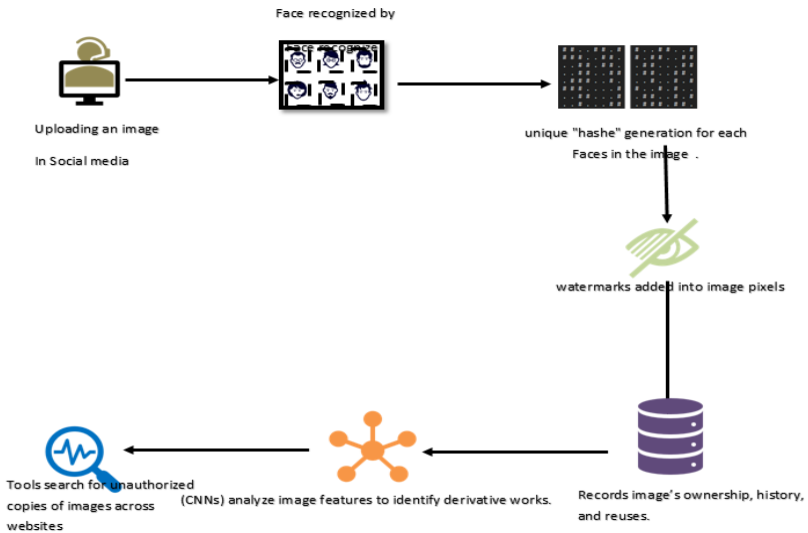


Fig 3: Process control flow of proposed system

IV. Technological Aspect

A) Face Recognition Application

Facial Recognition Application is a software that is used before posting the media (image or video) in the social media platform to analyze and recognize objects and faces of an image . It identifies the facial angles, alignments, patterns, and other facial features. The process begins with capturing an image or videos and detecting the image. After that the software detects the presence of the face in the image apart from the background and other objects and the algorithm separates the face from every other things. Once a face is detected , the software aligns its standardized format which is done by locating key points such as the position of eyes ,nose , mouth , eyebrows and adjusting the face so that is can be analyzed consistently. Then the Feature Extraction software analyzes the face to extract distinct features, which include the distance between the eyes , the texture of the skin, contour of the lips . The system use deep learning models to generate 'faceprint' , a unique set of features .

B) Image Hashing

Image Hashing is a technique used to create a unique fingerprint or signature or ID of an image which allows a comparison and identification of images. In this process, the image is converted into the hash (a fixed-size string of characters represented in hexadecimal characters) which represents the content of the image. When a new record is created in the social media (e.g. post) the database management system generates a unique ID. Also with that , after the image processing with resizing, normalizing the key features are extracted like color distributions, and pixel intensity with different hashing algorithms. The extracted feature (mainly the faces of the image) is used to generate a hash value using various hashing algorithms like Average Hash which is also known as aHash , Perceptual Hash which is known as pHash , Difference Hash which is known as dHash. The Hash values are unique and used to find the similarity and differences between another images . Hash values can be used to identify the duplicate or near duplicate images in the

vast dataset. Hash values is used for copyright enforcement as hashing allows fast and efficient image comparisons. Hash values are much smaller in size (MD5 produces 128-bit hash value , SHA-1 produces 160-bit ,SHA-256 produces 256-bit and SHA-512 produces 512-bit hash value).

C) Invisible Watermarking and Invisible Fragile Watermarking

Watermarking is a technology used to protect the digital contents or images such as images or videos. It is a hidden identifier which is embedded into the digital contents or images which is used to have the ownership of the image preventing alternation of the image . It is typically consists of a unique code or identifier which can be used to trace the origin of the content if it is shared or distributed without owner's permission.

In this software, invisible watermarking and inviable fragile watermarking is used in each and every face images as an evidence of ownership.

The **invisible watermark** should neither be noticeable to the viewer nor degrade the quality of the content , Invisible watermarks are desirable to design a watermark whose decoder is scalable with every generation of computer . Invisible Watermarks are designed to be unchanged to the common modifications like compression , scaling ,cropping and even screenshots . Even if the content gets altered the watermark will be detectable and unchanged . Invisible watermarks can help to identify the source of leaked contents making to easier to trace and allows the owner to monitor the usages of their content across the internet.

The **Invisible Fragile Watermarks** are also hidden and not visible to the viewers , Invisible fragile watermarks are used to detect tampering or unauthorized modifications of the content . Invisible fragile watermarks in applies to sensitive documents to ensure they remain unchanged. It does not affect the visual quality of usability of the content.

The combination of Invisible Watermarks and Invisible fragile watermarks can be used to enhance the security of the

image content . The image content can be embedded with both Invisible watermarks and Invisible fragile watermarks . Invisible fragile watermarks can check the integrity ,flagging , alternation , tempered or not where as Invisible watermarks can provide ongoing identification and ownership information.

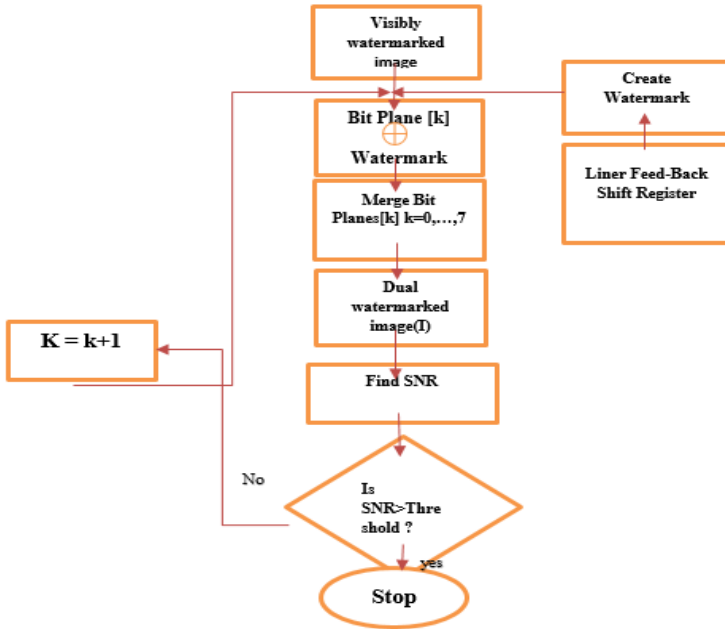


Fig 4: Representation of Invisible Watermark insertion process

D) Storing in Database

Extracted data will be stored in a database managed by the social media database, which is a database schema . Database Management Systems uses Relational Database as a structured table to store and manage data (e.g. MySQL, PostgreSQL etc). Unstructured or semi -structured data is handled by NoSQL (e.g. MongoDB , Redis etc.) which is well- suited for large-scale applications. Databases use indexing to improve the speed of data retrieval. Replication will be used to create multiple copies to database across different servers.

E) AI - Image Detection

After string all the data, if further a content is needed to be tracked, whether it could be a screenshot , Ai Image Detection will be used to detect the image . After comparing the data and image's watermarks with the stored database , the contents source and shared locations will be detected very easily.

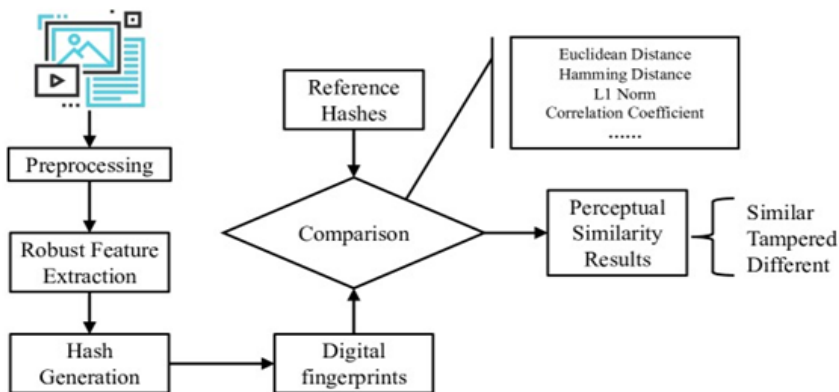


Fig 5 : Framework of digital fingerprinting systems

Conclusion

We conclude future scope of improvement in the concept domain as follows –

- This system will also track the video content and recognize the reuse of unauthorized content, which will ensure the complete privacy to the social media users .
- Future works will focus on improving the efficiency and scalability of the framework.
- This system will enhance the privacy to the world wide public social media platforms reducing the cyberbullying cases .

With the above observations, this research contributes to the ongoing efforts to develop secure and privacy preserving facial reusage ,and more ethical use of data in law enforcement.

References

Digital Watermarking : A Tutorial Review Saraju P. Mohanty Dept of Comp Sc and Eng. University of South Florida Tampa, FL 33620

Modeling, obtaining and storing data from social media tools with Artefact-Actor-Networks Wolfgang Reinhardt, Tobias Varlemann, Matthias Moi and Adrian Wilke University of Paderborn 33102 Paderborn, Germany

IPM-Model: AI and metaheuristic-enabled face recognition using image partial matching for multimedia forensics investigation with genetic algorithm

Leon O. Chua, "CNN: A Vision of Complexity", **International Journal of Bifurcation and Chaos**, Vol. 07, No. 10, pp. 2219-2425 (1997)

Wolfgang Reinhardt, "Modeling, obtaining and storing data from social media tools with Artefact-Actor-Networks", Research Gate (Jan 2010)

"Alarming Cyberbullying Statistics!", Impulsec, <https://impulsec.com/cybersecurity-news/cyberbullying-statistics/> (2025)

Digital Watermarking : A Tutorial Review Saraju P. Mohanty Dept of Comp Sc and Eng. University of South Florida Tampa, FL 33620.

Boddeti, V.N. Secure face matching using fully homomorphic encryption. In Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22-25 October 2018; pp. 1-10. [Google Scholar]

Y. LeCun, B. Boser, J. S. Denker, D. Henderson, R. E. Howard, W. Hubbard, and L. D. Jackel. Backpropagation applied to handwritten zip code recognition. *Neural Computation*, 1(4):541-551, Dec. 1989. 2, 4

Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval. Simple functional encryption schemes for inner products. In *Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography*, Gaithersburg, MD, USA, March,

30April 1, 2015, Proceedings, pages 733–751. Springer,2015. 2
https://github.com/ageitgey/face_recognition

Olden, M., Holle, R., Heid, I.M. and Stark, K.: IDGenerator: unique identifier generator for epidemiologic or clinical studies. BMC Med. Res. Methodol. 16, 1–10 (2016). <https://doi.org/10.1186/s12874-016-0222-3>

Chang Huang, Shenghuo Zhu, and Kai Yu. Large scale strongly super-vised ensemble metric learning with applications to face verification andretrieval. arXiv preprint arXiv:1212.6094, 2012

ZHOU, S., KRUEGER, V., AND CHELLAPPA, R. 2003. Probabilistic recognition of human faces from video. Comput. Vis. Image Understand. 91, 214–245.

Nie Ruihua, Li Kingman, Shi Ting, Research on Information Security in Face Recognition System, Digital Technology & Application. 37 (11) (2019), p. 167.

PENG F, QIN L, LONG M. Face presentation attack detection using guided scale texture, Multimedia Tools and Applications. 77(7) (2018), pp. 8883-8909.

Liu, Xiaoming, and Tsuhan Chen. “Video-based face recognition using adaptive hidden markov models.” Computer Vision and Pattern Recognition, 2003. Proceedings. 2003 IEEE Computer Society Conference on. Vol. 1. IEEE along with SVD coefficients.” (2008).

I. Damgård, M. Geisler, and M. Krøigård. A correction to “efficient and secure comparison for on-line auctions”. Cryptology ePrint Archive, Report 2008/321,2008. <http://eprint.iacr.org/2008/321>.

F. Armknecht and A.-R. Sadeghi. A new approach for algebraically homomorphic encryption. Cryptology ePrint Archive, Report 2008/422, 2008. <http://eprint.iacr.org/>.

O. Bowcott. Interpol wants facial recognition database to catch suspects.Guardian (October 20, 2008), <http://www.guardian.co.uk/world/2008/oct/20/interpol-facial-recognition>.

D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella. Fairplay — a secure two-party computation system. In USENIX, 2004. <http://fairplayproject.net>.

P. Jonathon Phillips Support Vector Machines Applied to Face Recognition. National Institute of Standards and Technology.

Qiang Zhu, Shai Avidan, Mei-Chen Yeh, Kwang-Ting Cheng Fast Human Detection Using a Cascade of Histograms of Oriented Gradients. Proceedings of the 2006 IEEE Computer Society Conference on Computer Vision and Patter Recognition. 2006.

Xiaopeng Yang, Hui Zhu, Rongxing Lu, Ximeng Liu, and Hui Li. Efficient and privacy-preserving online face recognition over encrypted outsourced data. In IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData), iThings/GreenCom/CPSCoM/SmartData 2018, Halifax, NS, Canada, July 30 - August 3, 2018, pages 366–373. IEEE, 2018. 2