Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/4/2023303

A secret image sharing solution for autonomous vehicles

Zuyu Li

Northeastern University, Khoury College of Computer Sciences,Boston, USA

li.zu@northeastern.edu

Abstract. With the improvement of personal privacy awareness and government agencies' awareness of national security information protection, data access and data security of smart cars is a thorny problem. The fundamental reason is that the key to access and store data is kept in the hands of smart car companies. Although many scholars have made great progress in the research of secret image sharing solutions before, such as progressive visual secret sharing, polynomial based secret image sharing, etc., these encryption schemes are single key encryption and cannot solve the technical problems encountered by the current autonomous vehicle. Therefore, based on the research of previous scholars and taking into account the social problems in solving the existing image sharing, this paper proposes two secret image sharing solutions. One is key sharing solution; The other is Images Sharing solution. Through the theoretical analysis of the application scenario, we can conclude that these two solutions can well solve the problems of whether users, smart car companies or third-party institutions infringe on users' privacy, whether it is due to the security hidden dangers brought by smart car technology, and whether they violate the national information security law.

Keywords: data security, secret image sharing, automatic driving, data transmission.

1. Introduction

From the birth of the world's first radio-controlled car, the "Linriccan Wonder," to the introduction of the Mercedes-Benz vision-guided robot Van in 1980, autonomous driving technology has advanced significantly in just a few decades. Technologies such as adaptive cruise control, lane parking, and steering assistance have become iconic of modern autonomous driving technology [1]. Self-driving vehicles are gaining popularity because self-driving technology has the potential to significantly minimize the risk of collisions. Around 3,500 people are killed in road accidents in Germany each year, according to reports, and more than 300,000 are wounded, many of them badly. According to relevant department data, 90 percent of these incidents are the result of human mistake [2]. And, as long as the self-driving vehicle is designed properly, it cannot go wrong. The more sophisticated these self-driving technologies get, the more complicated traffic scenarios they are capable of recognizing, calculating, and grasping. According to insurance statistics, automated emergency braking assists in reducing rear-end crashes by 38%, lane maintaining assists in reducing accidents by 4.4%, and lane change assists in reducing accidents by 1.7% [3]. In the United States, authorities performed an extensive investigation of collisions between 2005 and 2007 and discovered that at least one vehicle was hauled from the site. As a result, they determined that 94 percent of incidents were caused by driver mistake or physical condition [4]. If automation could completely eliminate all automotive accidents caused by driver error, autonomous technology would save thousands of lives each year [5]. According to the Insurance Institute for Highway Safety's (IIHS) analysis of 2014 accident statistics,

DOI: 10.54254/2755-2721/4/2023303

the largest overall benefit would be a 17% decrease in crash deaths if all interstate kilometers were driven completely by automation and no vehicle crashes were reported. Collision damage was decreased by 9% [6]. Combining the aforementioned facts, it's easy to understand how autonomous cars will contribute to traffic accident reduction in the future.

Additionally, autonomous driving enables drivers and passengers to make better use of their time in the automobile. For instance, Audi CEO Rupert Stadler has said that clients may utilize this time for relaxation, enjoyment, and viewing movies, among other activities, by using highly automated and self-driving technologies [7]. Damien Scott, chief commercial officer of Renovo.auto, added: "Systems like as CarPlay, Android Auto, and Microsoft Sync have all aided in the integration of this material into the automobile system, and the content is now mostly audio." The subsequent step will be more straightforward. Utilize the vehicle's unique content possibilities, particularly those related to visual material. Thus, with highly autonomous cars, the passenger experience may be designed on a huge screen. This has the potential to increase the amount of visual material available on car screens through cellphones. To begin, techniques such as Apple AirPlay and Google Casting will make cellphones the major source of content for such displays. Local storage and content will become more prevalent as cars develop. For instance, popular entertainment will be put on the car based on public demand [8]." Without a doubt, once L4 or L5 autonomous driving technology is widely adopted and accepted by consumers, the primary differentiator for devices such as in-vehicle electronics will be the driver's entertainment experience, creating new opportunities for online audio and entertainment companies to innovate [9].

Nowadays, the vehicle business has undergone dramatic changes, with "intelligence," "network connectivity," "sharing," and "electricity" becoming industry buzzwords. Among them, the excitement of the top automobile manufacturers for "intelligent" is exceptional, and customers are also daring enough to experiment with automobile "intelligence." Due to the market and industry's contradictory motivations, major automobile manufacturers have boosted their investment in the area of autonomous driving. For instance, Toyota Motor, a long-established international corporation, intends to spend 20 billion yen in Woven, a software subsidiary focused on autonomous driving, car operating systems, and high-definition mapping. It encompasses all automotive digital enterprises, including as intelligent driving, intelligent cockpit, and digital marketing platforms; and Audi, Honda, GAC, and WM Motor, among others, have advanced the mass production of L3 autonomous driving [10]. We can plainly see that conventional top automobile firms and certain Internet giants are investing heavily in autonomous driving technology, indicating that whoever develops a really self-driving vehicle will be able to conquer the Internet in the next age.

If 10 years ago, the reason for limiting the popularity of self-driving cars was "technology," I think the current one is "data security." Access to data security in electric cars and other connected vehicles continues to be a sensitive issue. This is partially due to the fact that the data access key is a single key that Tesla and other autopilot companies closely guard. This means that manufacturers of self-driving cars retain total control over the use of cameras to collect road data and the unintentional collecting of pedestrian data while driving. Without clearance from Tesla, no one has the authority to access this data. Similarly, if Chinese authorities desire to examine if these data are safe and whether they are covertly transported back to the United States, Tesla would decline the request on the basis of "personal privacy," leaving the officials with no method to assure the data's security. Guan Xuejun, President of China's automotive selection network, expressed concern over Tesla's radars and probes precisely because Tesla's whole transmission system is interconnected with the US military's infrastructure. Once a significant number of critical personnel acquire Tesla, all secret material will be automatically forwarded to the US military [11]. Following that, the Chinese military imposed a restriction, requiring Tesla owners and military families to park their cars outside the military zone. The military is worried that the American electric vehicle manufacturer obtains sensitive data in ways that are beyond its control through built-in cameras and hence cannot ensure the ultimate safety of military secrets [12-13]. Although Elon Musk said that Tesla has established data centers in China to facilitate data localization, all data generated by automobiles sold on the Chinese mainland would be stored in China [14-16]. This, however, has not allayed the anxieties of the Chinese government and people.

DOI: 10.54254/2755-2721/4/2023303

On the other hand, if Tesla unilaterally retains the decryption key and the user requests car data as a result of a car accident or vehicle failure, and the data are unfavorable to Tesla, such as as a result of system failure or program hacking, the company may deny the user access to this portion of data for ostensibly legitimate reasons. Additionally, this will obstruct the administration of justice. According to speculations, a dissatisfied buyer climbed onto the roof of a Tesla during the April 2021 Shanghai car show to protest the corporation. The business refused to furnish her with information on her father's car, which was involved in a crash as a result of "brake failure" [17]. While Tesla has developed a number of new tools to allow consumers to view their vehicles' data, these efforts do not allay public concerns about data erasure or manipulation by automotive computers.

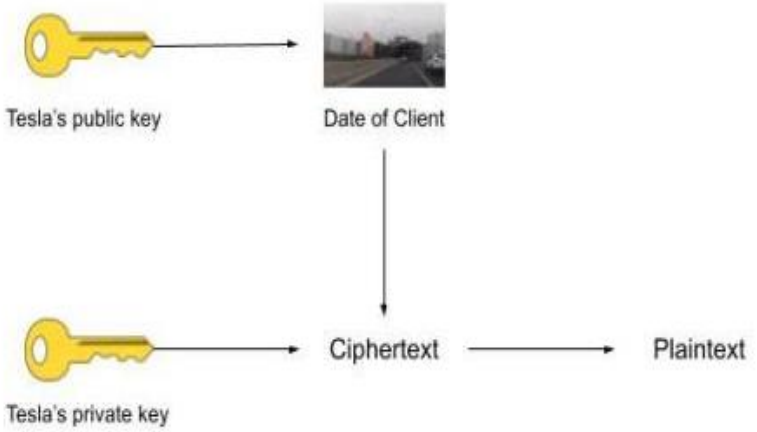

Figure 1. Tesla single key decryption process.

This paper proposes an autopilot data and image sharing technique based on this. The goal is to encrypt the image of the data obtained by the smart car camera and divide the key into three parts: one for Tesla, one for the user, and one for the government or a trustworthy third party. To decode the image data, anybody or any organization must get two of the three keys. The information cannot be decrypted without the cooperation of at least two individuals. The second half of this article will review many contemporary approaches for secret image sharing; the third section will investigate and detail the strategy proposed in this study; and the fourth part will analyze the application scenarios of the encryption system proposed in this paper; and the fifth section will conclude this work.

2. Background

2.1.Visual Secret Sharing

In 1994, Naor and Shamir [18] devised this approach. They degrade an image into n meaningless transparencies on average. To prevent data leakage, the VSS encryption algorithm splits the secret image into M-pixel blocks, each of which contains an equal number of randomly distributed black-and-white pixels and their corresponding share [19]. Due to the fact that the chance of seeing black pixels in a transparency is equal to the probability of seeing white pixels, no secret information can be recovered from any transparency. Then distribute the transparencies to each member of the group. Before the secret information may be exposed during decryption, at least k transparencies or more shares must be stacked. If not, it will stay unencrypted. Which have been dubbed "threshold schemes" [20]. Additionally, a rising number of professionals provide a variety of secret sharing strategies based on traditional VSS technology. For instance, Wu and Chen [21] developed an encryption approach that converts two secret pictures into two meaningless shared images a and B. Wu and Chang [22] improved the technical system developed by Wu and Chen.

However, the above-mentioned picture encryption method, which is based on VSS image encryption, has the following disadvantages [23]:

DOI: 10.54254/2755-2721/4/2023303

1. The human eye cannot notice the concealed image recreated in ordinary VSS due to its low contrast. The more concealed photos traded, the more contrast is lost;

2. There are concerns with pixel expansion, which increases the cost of sending concealed photos;

3. There are concerns with pixel alignment during the secret decoding process.

2.2.Progressive Visual Secret Sharing

Certain scholars have proposed two ways for progressive visual secret sharing technology: the first is to encrypt the whole secret image [24,25,26]; the second is to encrypt the secret image based on the image block [27]. The first method encrypts and decrypts the whole secret image. This strategy entails stacking several shares on top of the overlay image, which proportionally raises the contrast of the reconstructed image. As a consequence, the secret image will be unveiled gradually. Another possibility is to divide the secret image into several non-overlapping image parts. By superimposing a shared image on the stacked image, additional image blocks that were before concealed become visible. Additionally, this method may be used to retrieve the concealed picture.

However, this kind of encryption does have several downsides [28]:

1. Each matrix in these common models must be designed uniquely, increasing the scheduling matrix's complexity and complicating the method's implementation.

2. As the number of participants increases, so does the rate of pixel growth.

3. Due to the absence of contrast in the reconstructed image, it is more difficult to distinguish the contents of some buried blocks.

2.3.Progressive Visual Secret Sharing

Chen and Lin [30] proposed a way for modifying the H threshold RI based on Thien and Lin's approach [29]. (1 I h). Their approach starts by extracting R (r = R 1 + R 2 +... + R H) pixels from the concealed image simultaneously. Gray values are reordered in pixels according to their bit plane order, beginning with the most significant bit and ending with the least significant bit. Finally, a replication of the freshly calculated R value is performed. Wang and Shyu [31] also use the importance of the different bit planes to divide the gray value of the picture into J plane groups in order to do progressive secret sharing. Yang and Huang [32] and Yang and Chu [33] established a strategy for developing a (k, n) scheme with threshold properties and scalability. The amount of data included in a decrypted secret is related to the number of shadows used in the decryption procedure. Certain shadows, according to Li et al. [34], may be more important than others.

However, all shares in the previous system are obtained by solving polynomials using Lagrange interpolation. As a consequence, these systems are incapable of immediately deciphering hidden images through stacking and sharing. Computers are essential for classified information recovery [35]. As a consequence, venture capital does not follow these processes.

2.4.Secret image sharing scheme based on sharing matrix and image encryption

In contrast to most of the approaches discussed above, Bao Long et al. [36] suggested a lossless (k, n) secret image sharing method (smie-sis) based on the combination of a sharing matrix and image encryption. The author argues that the model incorporates a chaos-based encryption method and a shared coding technique that may significantly lower the cost of shared block reconstruction and is applicable to binary, grayscale, or color pictures. Additionally, it has a low pixel expansion ratio, which is advantageous for lowering storage and transmission costs. Additionally, SMIE-SIS provides a high level of protection against brute-force assaults, differential attacks, and a system for identifying fraudulent shares.

DOI: 10.54254/2755-2721/4/2023303

3. Proposed encryption system scheme

3.1.Key sharing solution

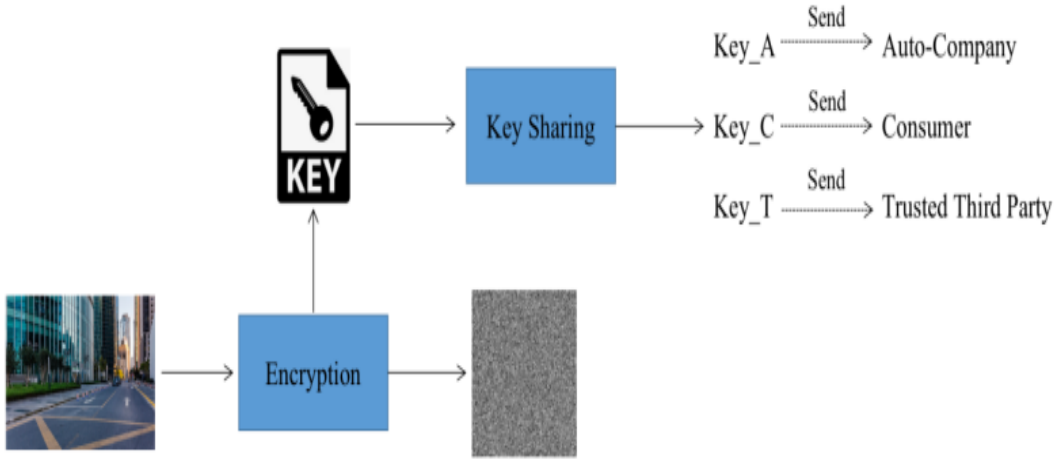

Figure 2. Encryption solution based on key sharing.

The encryption solution based on key sharing is to encrypt the original information data to generate encrypted images and an original key. After the original key is processed by the key sharing system, three keys will be output, which are key_A, key_C and key_T, and then distributed to auto company, consumer and trusted third party for independent storage.

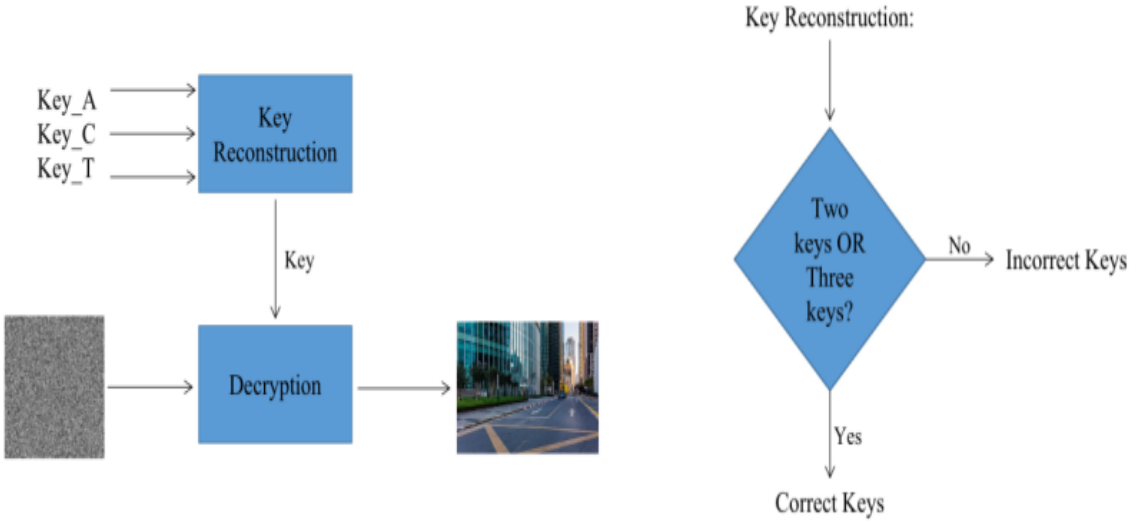

Figure 3. Decryption process of encryption solution based on key sharing.

The decryption process of this scheme first needs to verify the decryption key through key reconstruction. If the check result is incorrect or the share of decryption key is less than 2, the decryption operation cannot be performed. On the contrary, if the check result meets the decryption conditions, the key reconstruction system will combine these keys into a new key and input it into the image decryption system, and then the system will restore the encrypted image to the original image.

DOI: 10.54254/2755-2721/4/2023303

3.2.Images sharing solution

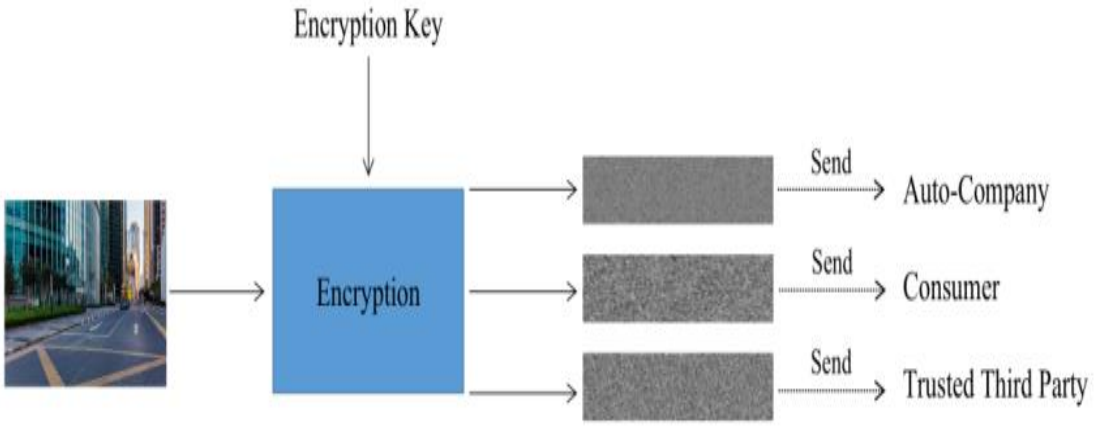

Figure 4. Encryption solution based on image sharing.

Encryption solution based on image sharing is to output three encrypted pictures EA, EC and ET. After the original image is encrypted by the encryption system, then send them to auto company, consumer and trusted third part for safekeeping.

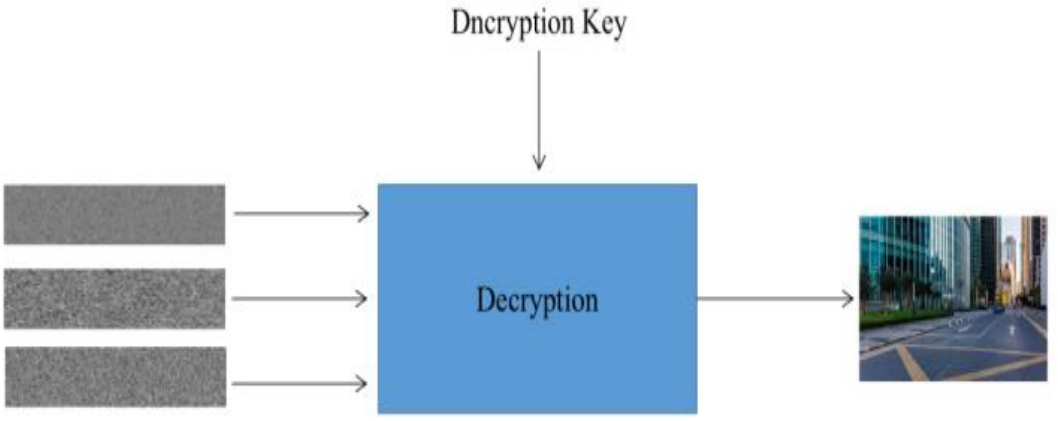

Figure 5. Decryption process of encryption solution based on image sharing.

In order to obtain the original picture information, the scheme needs to input three encrypted pictures into the decryption system for decryption at the same time.

4. Deployment and data transmission

If we wish to install any of the above two systems, we must decide whether to distribute the encrypted secret images locally or on the cloud. If the encryption is performed locally, the user is immediately presented with three encrypted noise images, from which he or she may pick brute force cracking to retrieve the matching decoded original images. This is in direct conflict with the original objective of our system's design. To address this issue, I propose that the noise images provided to the trustworthy third party and the business be re encrypted at the local end using the third party's and the company's public key signatures, and then disseminated. If you wish to upload the gathered photographs to the cloud and distribute the noisy images after encryption, you must encrypt the original images transferred to the cloud to avoid intermediary interception. After encrypting the original data in the

DOI: 10.54254/2755-2721/4/2023303

cloud, it is essential to sign and encrypt using the three parties' public keys prior to delivery. This is also to prevent information from being intercepted by middlemen.

5. Scenario analysis

First, antecedents and consequences of the accident are not the same, in a single key system, if the key is kept by the autonomous vehicle company, then the accident will happen if the vehicle accident occurs due to technical defects. The company may not actively disclose information and images to help the law enforcement agencies to sort out the causes and consequences of the accident. For consumers, because of money, material resources, manpower and other reasons, they are in a weak position against automatic driving companies. Therefore, based on the above factors, the road of protecting consumers' rights is bound to be very long. If the encryption system recommended in this paper is deployed, the legal disputes caused by car accidents can be well solved. Because consumers can complain to the court that the automatic driving company intends to hide the truth and apply to China's network security department for decryption of the image. After the relevant qualification is approved, the key of the trusted third party and the key in the user's hand will jointly unlock the encrypted image. Similarly, if enterprises are maliciously framed by consumers - attributing the accidents caused by their own improper operation to the problems of the technology itself, enterprises can also apply to the court and the network security department to jointly unlock the encrypted image. Therefore, if this scheme can be successfully deployed, both enterprises and consumers can reduce the cost of safeguarding their rights and safeguard their own interests in time.

Second, if the single key is kept by Tesla's non China self driving automobile companies, China will surely worry that these car cameras will collect government unit information and military confidential information and limit the entry of foreign auto driving vehicles into the above areas. Secondly, as the world's leading enterprise in the field of new energy and automatic driving, Tesla certainly does not want to easily give up the Chinese market because of information and image security. Then, if the encryption scheme proposed in this paper is deployed, even if Tesla wants to transmit data or the U.S. government requires it to transmit data back to the United States, all data cannot be transmitted out of China without a third party or user's key. On the whole, once the scheme is successfully deployed, it can solve the Chinese government's concern about road information leakage. For foreign smart car companies, once the problem of potential information leakage is solved, they can also take a share in the world's largest automobile consumer market.

Third, if the single key is kept in the hands of the user, once the user dies due to an accident, the image information recording the truth may no longer be made public. This will be a very big adverse factor for law enforcement agencies to effectively sort out specific cases and make corresponding judgments, and smart car companies to maintain and optimize their products. If the encryption system designed in this paper can be successfully applied, even if the user dies due to a traffic accident, as long as the court makes a decision according to law to allow decryption with the key held by the smart car company and China's network security department, the cause of the traffic accident may still be found by decrypting the image.

Fourth, if the single key is kept by the Chinese network security department, that is, a third party, it will involve the problem of user privacy. Because some users may worry that the government may infringe their privacy by privately invoking the information collected by their car cameras without their consent. If the encryption system scheme of this paper is deployed, there is no need to worry about such problems, because the lack of any key can not decrypt the encrypted image.

6. Conclusion

The research results of this paper show that one of the problems why autonomous vehicle are difficult to be accepted by the public and government agencies is that intelligent vehicle companies are difficult to deal with the privacy and security of the data collected during the driving process. For example, the Chinese government departments mentioned in this article have banned almost all Tesla cars from entering. Based on these situations, this paper puts forward the encryption schemes of Images Sharing solution and key sharing solution on the basis of the research results of secret images sharing of many previous scholars and the problems faced by automatic driving technology in the world. Through the

DOI: 10.54254/2755-2721/4/2023303

rigorous and detailed analysis of the security of complex application scenarios and image data encryption, we can find that these two schemes can well solve the problems brought by smart car companies, users or third-party institutions.

References

[1] B Keshav. Autonomous cars: Past, present and future a review of the developments in the last century, the present scenario and the expected future of autonomous vehicle technology. In 2015 12th international conference on informatics in control, automation and robotics (ICINCO). Vol. 1, pp. 191-198, July 2015.

[2] Most Common Cause of Serious Traffic Accidents. http://www.versicherungsjournal.de/versicherungen-und-finanzen/die-haeufigsten-ursachen-von-schweren-verkehrsunfaellen-126342.php

[3] Brenner, W., & Herrmann, A. An overview of technology, benefits and impact of automated and autonomous driving on the automotive industry. Digital marketplaces unleashed. pp. 427-442, 2018.

[4] Singh, S. Critical reasons for crashes investigated in the national motor vehicle crash causation survey (No. DOT HS 812 115), 2015.

[5] Mueller, A. S., Cicchino, J. B., & Zuby, D. S. What humanlike errors do autonomous vehicles need to avoid to maximize safety?. Journal of safety research, Vol. 75, pp. 310-318, 2020.

[6] Robot cars won't retire crash-test dummies anytime soon. https://www.iihs.org/news/detail/robot-cars-wont-retire-crash-test-dummies-anytime-soon

[7] Handelszeitung. https://www.handelszeitung.ch/unternehmen/rupert-stadler-wir-muessen-audi-neu-erfinden-1014060

[8] Analysis of the future development of in-vehicle entertainment in the era of autonomous driving. https://zhuanlan.zhihu.com/p/36135288

[9] Frauenhofer-Institut. https://blog.iao.fraunhofer.de/images/blog/studie-value_of_time.pdf.

[10] Self-driving decisive battle for the commanding heights of future cars. http://www.xinhuanet.com/techpro/2021-03/26/c_1127256866.htm

[11] The Cyberspace Administration of China and other departments interviewed Tesla, public opinion said the product endangered national security. https://www.rfa.org/mandarin/yataibaodao/ql-02102021042949.html

[12] China reportedly bans Tesla cars from military facilities over spying fears. https://www.engadget.com/china-military-bans-tesla-cars-162136546.html

[13] China to Restrict Tesla Use by Military and State Employees. https://www.wsj.com/articles/china-to-restrict-tesla-usage-by-military-and-state-personnel-11616155643

[14] Tesla: Has built a data center in China to localize data storage. https://www.yicai.com/news/101061768.html

[15] Tesla opens new China research, data centers; will store data locally. https://www.reuters.com/business/autos-transportation/tesla-opens-new-china-research-data-centers-will-store-data-locally-2021-10-25/

[16] Tesla will store Chinese user data locally, following Apple ' s suit. https://techcrunch.com/2021/05/26/tesla-china-user-data-storage/

[17] Tesla's monthly sales in China hit a new high, but data security is still a hidden danger. https://www.fortunechina.com/shangye/c/2021-10/13/content_398938.htm

[18] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology-EUROCRYPT ' 94, LNCS. Springer-Verlag, Vol. 950, pp. 1 – 12, 1995.

[19] Hou, Y. C., Quan, Z. Y., Tsai, C. F., & Tseng, A. Y. Block-based progressive visual secret sharing. Information Sciences, Vol. 233, pp. 290-304, 2013.

[20] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology-EUROCRYPT ' 94, LNCS. Springer-Verlag, Vol. 950, pp. 1 – 12, 1994.

DOI: 10.54254/2755-2721/4/2023303

[21] C.C. Wu, L.H. Chen. A study on visual cryptography, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.
[22] Wu, H. C., & Chang, C. C. Sharing visual multi-secrets using circle shares. Computer Standards & Interfaces, Vol. 28(1), pp. 123-135, 2005.
[23] Chen, T. H., & Wu, C. S. Efficient multi-secret image sharing based on Boolean operations. Signal Processing, Vol. 91(1), pp. 90-97, 2011.
[24] Chen, S. K. Friendly progressive visual secret sharing using generalized random grids. Optical Engineering, Vol. 48(11), pp. 117001, 2009.
[25] Fang, W. P. Friendly progressive visual secret sharing. Pattern recognition.,Vol. 41(4), pp. 1410-1414. 2008.
[26] Hou, Y. C., Quan, Z. Y., Tsai, C. F., & Tseng, A. Y. Block-based progressive visual secret sharing. Information Sciences, Vol. 233, pp. 290-304, 2013.
[27] Wang, R. Z. Region incrementing visual cryptography. IEEE Signal Processing Letters, Vol. 16(8), pp. 659-662, 2009.
[28] Hou, Y. C., Quan, Z. Y., Tsai, C. F., & Tseng, A. Y. Block-based progressive visual secret sharing. Information Sciences, Vol. 233, pp. 290-304, 2013.
[29] Thien, C. C., & Lin, J. C. Secret image sharing. Computers & Graphics, Vol, 26(5), pp. 765-770. 2002.
[30] Chen, S. K., & Lin, J. C. Fault-tolerant and progressive transmission of images. Pattern recognition, Vol. 38(12), pp. 2466-2471. 2005.
[31] Wang, R. Z., & Shyu, S. J. Scalable secret image sharing. Signal processing: Image communication, Vol. 22(4), pp. 363-373, 2007.
[32] Yang, C. N., & Huang, S. M. Constructions and properties of k out of n scalable secret image sharing. Optics Communications, Vol, 283(9), pp. 1750-1762. 2010.
[33] Yang, C. N., & Chu, Y. Y. A general (k, n) scalable secret image sharing scheme with the smooth scalability. Journal of Systems and Software, Vol. 84(10), pp. 1726-1733, 2011.
[34] Li, P., Yang, C. N., Wu, C. C., Kong, Q., & Ma, Y. Essential secret image sharing scheme with different importance of shadows. Journal of Visual Communication and Image Representation, Vol. 24(7), pp. 1106-1114, 2013.
[35] Hou, Y. C., Quan, Z. Y., & Tsai, C. F. A privilege-based visual secret sharing model. Journal of Visual Communication and Image Representation, Vol. 33, pp. 358-367, 2015.
[36] Long B , Shuang Y , Zhou Y . Combination of Sharing Matrix and Image Encryption for Lossless (k,n) -Secret Image Sharing. IEEE Transactions on Image Processing , Vol. 26(12), pp. 5618-5631, 2017.