*Recursive threshold Visual Cryptography for data security during vehicle to vehicle connectivity*

Shiva Saketh Mahagosaiwar, Aravind Reddy Etikala, Kishore Kumar Sreerama, Arjun Saranga (Team Titans)

Department of Computer Science

Kent State University

Kent, USA.

***Abstract*—Vehicle to vehicle connectivity plays a key role in future when unmanned vehicles take over the roads of the world. Small range wireless transmission of data through Vehicular ad-hoc network such as source, path, speed destination, etc. must be shared between vehicles. The data shared must be secure if not they can be mishandled while sharing acquiescently. To protect the data most secure encryption type must be maintained to ensure the data privacy. Cryptography is the most prominent technique in maintaining the data security in which visual cryptography plays a major part. The proposed system uses recursive threshold cryptography for transmission and reception of data securely. This ensures effective data privacy at reduced cost. This technique can also be used in battle vehicles during war.**

***Keywords- v2v communication, cryptography, image, connectivity.***

1. INTRODUCTION

We are in a fast paced world, with smart technologies built to make our life easier and smoother. The Internet of Things is being integrated into the living spaces to make better connectivity and adaptability. Even the vehicles are not left behind; the vehicles are equipped with digital and smart equipment’s like sensors for automatic cruise control. Further expansion is happening to make the roads safer by developing vehicles which are able to communicate with each other by using some safe wireless technology available now. The automated cruise system although has the inherent limitation of not being able to communicate with the other vehicles around it. It can just see the vehicle in front, back and side and not assess anything beyond. Hence the role of Vehicle to vehicle communication is vital to implement smart technology. The technology thus implemented although should be secure. Hence the paper proposes the implementation of a recursive cryptographic method to secure the data transfer in terms of images. An intruder can change the data causing serious damage to life and vehicles as well, in a case when the V2V communicated is implemented for an automatic cruise control of a vehicle. Hence such attacks may be very threatening not only to property but also to human lives. Thus the prominence of securing the data transferred in a Vehicle to vehicle communication is inevitable for a safer society. The paper proposes the implementation of a recursive cryptographic algorithm to protect the data transfer from intruders.

1. VEHICLE TO VEHICLE COMMUNICATION

Vehicle-to-vehicle communication (V2V communication) is the wireless transmission of data between motor vehicles. The goal of V2V communication is to prevent accidents by allowing vehicles in transit to send position and speed data to one another over an ad hoc mesh network. Depending upon how the technology is implemented, the vehicle's driver may simply receive a warning should there be a risk of an accident or the vehicle itself may take preemptive actions such as braking to slow down.

V2V communication is expected to be more effective than current automotive original equipment manufacturer (OEM) embedded systems for lane departure, adaptive cruise control, blind spot detection, rear parking sonar and backup camera because V2V technology enables an ubiquitous 360-degree awareness of surrounding threats. V2V communication is part of the growing trend towards pervasive computing, a concept known as the Internet of Things (IoT).

In the United States, V2V is an important part of the intelligent transport system (ITS), a concept that is being sponsored by the United States Department of Transportation (DOT) and the National Highway Traffic Safety Administration (NHTSA). An intelligent transport system will use the data from vehicle-to-vehicle communication to improve traffic management by allowing vehicles to also communicate with roadside infrastructure such as traffic lights and signs. The technology could become mandatory in the not-too-distant future and help put driverless-cars on highways across America.

The implementation of V2V communication and an intelligent transport system currently has three major roadblocks: the need for automotive manufacturers to agree upon standards, data privacy concerns and funding. As of this writing it is unclear whether creation and maintenance of the supporting network would be publicly or privately funded. Automotive manufacturers working on ITS and V2V include GM, BMW, Audi, Daimler and Volvo.

Fig 2.1. Representation of connected vehicles

The Technology promises to solve that problem and provide a similarly more expansive perspective on traffic. It’s called V2V, which stands for vehicle-to-vehicle communications, and it basically employs a small radio transmitter and receiver on each vehicle that broadcasts information about its location, speed, and direction to other vehicles within several hundred yards. Unlike current radar, lidar, camera, and other sensors, it can know what oncoming vehicles are doing—or even those around corners and out of sight. The idea is to use this information to help electronic safety systems work more smoothly and safely. The hardware consists of an electronics package about as big as an Apple TV. This small box will house a radio transmitter and receiver, as well as a microcomputer. The radio operates in the 5.9-GHz band in a mode known as DSRC (Dedicated Short Range Communication systems).

Each vehicle will have a designated ID and will be connected to an onboard GPS system that can locate the vehicle’s position within a foot or two. The V2V systems will track a vehicle’s position and broadcast it, along with speed, direction of travel, and vehicle size, at a rate of 10 times per second. At the same time, the V2V systems will be receiving this same data from the other V2V-equipped vehicles around it. This data is then sent to the onboard computers that control and operate the electronic safety systems.

With very real concerns about electronic hacking and governmental or private tracking, security is a major priority of the V2V system. “The vehicle ID, along with the radio’s MAC address and the system’s security certificate will be changed every five minutes,” according to Jim Misener, the director of technical standards at Qualcomm Technologies, who is working with the Society of Automotive Engineers and an industry committee to develop the industry for V2V. Safety, of course, is the motivation for this technology. The reality is that the overwhelming majority of crashes are driver error of some sort—typically inattention, a failure to look around, or simply bad judgment.

A perfect example would be the ability to warn a driver proceeding towards an intersection with a green light that a car approaching on the intersecting road looks like it’s going to run the red light. None of the current safety aids would offer any help in avoiding such a dangerous T-bone crash. The warnings provided by the system would be determined by each vehicle manufacturer, just as they are today. They would include audible or verbal warnings, various lights or visual warnings in the instrument cluster or projected on the windshield, or vibration of the steering wheel or seat. NHTSA has been encouraging the development of V2V for years, but has yet to impose a mandate for its introduction. That’s expected in 2016, and the experts are guessing that NHTSA will require a gradual introduction of V2V devices beginning in the 2020 time frame. This will use the same hardware and communications standards to allow vehicles to communicate with smart traffic signals, roadway sensors to signal slippery conditions or heavy traffic, pedestrians in intersections, and more.

Some of the major research work carried out in this area is: To identify the potential threats of an attack, to specify architecture for securing the communication and to define the prerequisites for employing a cryptographic technique. Some of the research publications from the literature available are analyzed for finding the threats and the security architecture proposed in the literature are reviewed in the coming sections.

1. *Challenges in vehicle to vehicle communication*

The implementation of V2V communication network has to be carried out keeping some of the critical requirements in view. Privacy protection being one of the main issue. The communication should not contain any information that allows for identification of the individual through these messages. Secondly, the data transmission should be made secure by enforcing cryptographic encryption techniques. Thirdly, the communication network thus created should be made trustworthy by authenticating the users. Last, the system should be able to support the increase in traffic and also should be able to expand to cover the nation. Some of the attacks that may affect the user adversely can be: Bad decisions of driving that can cause traffic congestion, rerouting or even accident in worst case; the systems prone to error may be non-trust worthy by the users, and thus the acceptance may reduce over time.

1. TYPES OF ATTACKS ON VEHICLE TO VEHICLE COMMUNICATION

There are some potential threats that may be possible during inter vehicle data transfer are described briefly in this section:

If the intruder is able to compromise the credentials of the vehicle, there is every possibility to send messages on radio used for V2V communication to create and distribute message that may seem authentic but are misused for illegal purposes. The attacker can also manipulate or alter the data to mislead other vehicles for selfish intensions. The attacker can interfere with the message, interrupt or even deny the messages that are sent by the vehicles.

Type of attacks that can be launched on the communication system may be broadly categorized as: Privacy attacks and Framing attacks. The privacy attacks may lead to track the location of a person or the vehicle or the route of driving etc. The contents of the attack are misused here. The framing attack can report false complaints against a vehicle resulting in suspending the service of the vehicle from the system itself.

These attacks may seem to cause very minor harm to the system or vehicle, but potential intruders can create huge losses to life and property and even harm the society as well. As a solution to such attacks, the use of cryptographic encryption methods is a suitable choice in such scenarios and also inevitable. The paper proposes the use of image files to transfer data for inter vehicle communication. The image file must have the data in terms of fabricated values or garbage values. The actual data is encrypted in the image by using recursive threshold visual cryptography. The major advantage in this type of cryptography is that many data can be shared as parts in the pixels i.e. an image will contain only parts of a data which can be retained completely only if all the images are available and identifying the exact recursive pattern. It provides a double layer security to the data. The same technique can be used during war in battle vehicles. Consider two vehicles impending to strike their rival target. The vehicle should share position or location during the strike without the knowledge of their rivals. At this state for data security this type of technique can be used.

The data thus transferred, even if it is hacked, the possibility to decipher the data and read the original contents can take a long time if the latest methods of encryption are used. Thus most of cases, the intruder will fail to cause potential harm when there is a limited time available for the attack. The research paper here proposes the use of transferring the data in the form of encrypted images and use a recursive cryptographic encryption for the implementation. The security of such communication will require the design to ensure the following:

1. *Authentication*: Ensuring that the vehicle data is from a trustworthy user, and this has to be checked to prevent any spoofing or forgery
2. *Non repudiation*: The attacks causing denial of service has to be prevented
3. *Consistent flow*: The data flow should be consistent and regular to prevent any traffic or lag in the system causing the V2V communication to fail.
4. *Security*: The security of the life and property has to be ensured using the system

The hardware security can be ensured by implementing physical security measures on the vehicle, as this may be the only way to prevent an attack from an intruder who has a long time access to the systems. The software security of the system can be implemented which can be used to detect any attack or misbehavior. This can be false messages injected into the system or causing any malfunctioning of the vehicle. Hence cryptographic encryption has a crucial role to play in this scenario.

1. INTRODUCTION TO RECURSIVE INFORMATION HIDING USING VISUAL CRYPTOGRAPHY

One of the best methods to protect the data privacy, after the successful implementation of data security using the aforementioned methods is the classic ‘Cryptography’.It is a classic method of protecting the data by transforming the data into a form that can be understood only by the intended person. Though the transformation may result in a legible interpretation, the actual message remains hidden from any intruder. This process is called Encryption, and this method is called Cryptography. Here the intruder cannot decode the information, a process called deciphering if a key is not available. Hence this ensures data integrity to a certain extent depending on the size of the key. Smaller keys will offer a small protection and larger keys offers stronger protection from security threats. Although there is a possibility that the message is deciphered if the intruder manages to get the key, hence the key should be given limited access and it should be shared in a secure way to a minimal no. of entities. The key role of using encryption techniques is ensuring data security, confidentiality and data privacy. The security of the data from the intruders attack can be made infeasible by implementing Visual cryptography scheme.

The Visual Cryptography technique is a form of sharing information of confidential nature , that makes use of the human visual system itself to compute and analyze .This secret sharing scheme was invented by Blakley and Shamir but independently (Shamir,1979) and (Blakely,1979) . Further (Naor and Shamir, 1995) extended this concept to Visual Cryptography. Here the secret sharing scheme had a (k,n) threshold . The secret image that was to be shared is enciphered into ‘n’ random shares with no meaning, it was ensured that these individual share made no revelation about the original image, the deciphering of the secretly shared image could be carried out without any computation but by simple stacking of a minimum ‘k’ no. of share which is less than ‘n’. This traditional method of secret sharing had the inherent limitation of lower efficiency. That is any piece of random share could give at least (k/n) amount of information.

A brief literature review was carried out to see the available methods of image sharing using cryptography. Further improvement was carried out by Kak and Gnanaguruparan, 2002 in their paper, who proposed the concepts of Visual cryptography using recursive hiding of the information to be shared. They proposed the method of sharing the quantitatively smaller share within the shares of larger information. Here we see that the efficiency increased to almost cent percent. It was proposed as a non-recursive scheme. The scheme needs all the shares that were originally partitioned to decipher the secret. This idea was further developed to recursive threshold scheme but only forty percent efficiency was achieved as proposed in (Parakh and Kak, 2008). They further proposed a novel method to extend this scheme to protect the data stored online which increased the storage and bandwidth.

The major merit of the Visual cryptography scheme is the ability to decipher the image without any computational overhead. But this has few demerits. The growth in the number of share is exponential to the increase in shares. They need to produce a code book in advance of communication. This limitation is inherited in the recursive cryptographic method as well. Further development scheme was proposed by (Kafri and Karen, employs the use of random grids to combat with the existing drawbacks. Further (Shyu, 2009) followed by (Chen and Tsao, 2009) revised this scheme using random grids to a novel (n,n) scheme. This method claimed to improve the capability of secret information per bit without the need of generating code book. Each of the shares has the same size as that of the original image that had to be shared. This paper proposes a novel algorithm to improve the existing scheme using random grid and the experimental results are included to verify the performance of the scheme.

1. *Proposed Algorithm*

The method proposed in this report many number of extra images that are confidential are hidden in the portions of the larger images. The images to hire are arranged according to the order of increasing size, each time taking twice the secret size. This method can encipher each image into ‘m’ no. of cipher grids disordered, in such a way that all of these are needed to reveal the original hidden image. The algorithm is an implementation design for this proposed method.

The case considers 3 images to be hidden, say X, Y and Z with size l1 x b1, 2l2 x b2 and 2l3 x 2b3 respectively. The input to the algorithm is chosen to be ‘p’ no. of confidential images that needs to be transferred say C1,C2,C3,….Cp .here the size of the Cd th image should be taken as ld x bd , here 1≤ d≤ p , and also ld x bd should be equal to 2 ^(d/2)l1 x 2 ^[(d/2)-1] b1  and If ‘d’ is even, else 2^[(d-1)/2] l1 x 2^[(d-1)/2]b1

1. *The Algorithm:*
2. Select a random recursive function such that FG(a,b)  c, based on the random grid proposed in Kafri and Karen, which gives a random pixel ‘a’ as the input of the image to be hidden, and another pixel ‘b’ of the grid, and gives the result as pixel ‘c’ as the output of another grid
3. Create ‘n’ no. of partitions say F11, F21, F31……. Fn1 for the tiniest image to be hidden, say let it be C1

This can be accomplished by the following steps:

* Create random values of F11, F21, F31……. Fn-11 such that

for (1 ≤ k ≤ n-1; 1 ≤ i ≤ l1 and 1 ≤ j ≤ b1 ) ,

F11[i,j] = random (0,1)

* Produce random grid using FBn-2, using the values F11, F21, F31……. Fn-21

for (1 ≤ i ≤ l1 and 1 ≤ j ≤ b1 )

{ FB1[ i, j ] = FG (C1 [i, j], F11[i, j])

for ( 2 ≤ k ≤ n-2)

FBk[ i,j ] = FG (FB k-1[i, j], Fk1[i, j])

}

* Produce Fn1 by use of Fn-11 and FBn2,

for (1≤ i ≤ l1 and 1≤ j ≤ b1 )

Fn1[ i,j ] = FG (FB n-2[i, j], Fn-11[i, j])

3. for ( d =2 to ‘p’)

{ if ( d is even)

then goto Step IV )

else

goto Step V}

4. Produce some partitions for the image to be hidden Cd say, F1t, F2t, F3t……. Fnt  using the following procedure

* Create F1t, F2t, F3t……. Fn-2t  by placing these in first level of F2t, F3t… Fn-2t -1 and create a new level
* Generate a new random grid using the newly created level FGn-2t  using F1t, F2t, F3t……. Fn-2t
* Now place the Fn-2t -1 in the first level of Fn-1t  and also place Fnt -1 in the next level of Fnt
* Create new values of Fn-1t and Fnt  using FBn-2

5. Produce F1t, F2t, F3t……. Fnt  for the image to be hidden Cd as described

* Create F1t, F2t, F3t……. Fn-2t  by keeping the values F1t-1, F2t-1, F3t-1……. Fn-2t -1 in the first level of F1t, F2t, F3t……. Fn-2t respectively. Generate random values for next higher level of F1t , F2t , F3t……. Fn-2t
* Create random grid FGn-2 using F1t, F2t, F3t……. Fn-2t
* Place Fn-1t -1 in the first level of Fn-1t  and also place Fnt -1 in the level 2 of Fnt
* Create new values of Fn-1t and Fnt  using FBn-2

Here we see that the total information conveyed per bit of each partition of the pth confidential image is calculated to be: (2p – 1)/(2p-1n) bits. Hence we see that almost cent (100%) efficiency is obtained by using Recursive random grid cryptography for vehicle to vehicle communication.

1. RESULTS

We try to practically verify the scheme and find the efficiency of this algorithm taking three images that has to be kept confidential and shared. The sizes of these are taken as 70 x 70, 140 x 70, 140 x 140 .The figures are as shown below. Each of these are enciphered into three partitions of the same size as that of the image to be hidden as proposed in the algorithm. The images thus created are shown in the figure as well. The partition of the first and the second images are hidden in the part of the largest image i.e. the third one. The images thus created by overlaying the images one over the other are shown in the next figure. Thus we can see that the image to be hidden can only be deciphered if all the shares or partitions are available. Any less shares does not reveal any information about the enciphered image. Thus is very efficient method and maintains the privacy and confidentiality of the data to be transferred through images in a V2V communication.



Fig 5.1.Three figures of sizes 70 x 70, 140 x 70, 140 x 140 respectively

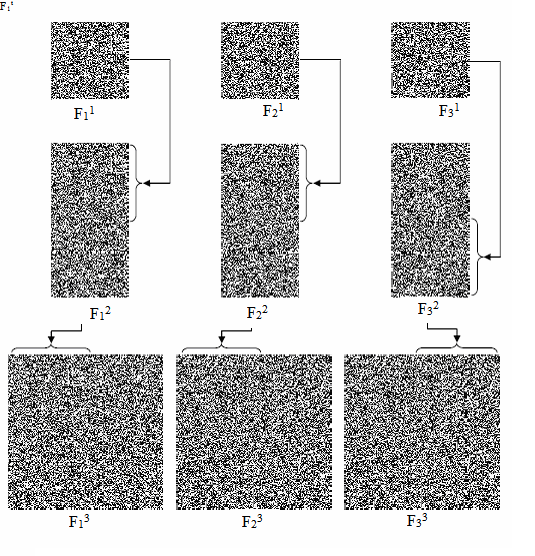


Fig 5.2. Recursive hiding of three secret images by random grids



Fig 5.3. Images generated by overlaying the partitions (a) Result of overlaying F11, F21 (b) Result of overlaying F21, F31, (c) Result of overlaying F11, F31, (d) Result of overlaying F11, F21, F31, (e) Result of overlaying F11, F22, (f) Result of overlaying F22, F32  (g) Result of overlaying F12, F32 , (h) Result of overlaying F12, F22, F32, (i) Result of overlaying F13, F23,, (j) Result of overlaying F23, F33 (k) Result of overlaying F13, F33 (l) Result of overlaying F13, F23, F33

REFERENCES

1. Xiubin Bruce Wang, Kai Yin, Xuedong Yan, Vehicle-to-vehicle connectivity on parallel roadways with large road separation, Transportation Research Part C: Emerging Technologies, Volume 52, March 2015, Pages 93-101, ISSN 0968-090X, retrieved from <http://dx.doi.org/10.1016/j.trc.2015.01.003>
2. Kai Yin, Xiubin Bruce Wang, Yunlong Zhang, Vehicle-to-vehicle connectivity on two parallel roadways with a general headway distribution, Transportation Research Part C: Emerging Technologies, Volume 29, April 2013, Pages 84-96, ISSN 0968-090X, retrieved from http://dx.doi.org/10.1016/j.trc.2013.01.005
3. Jose J. Tharayil, E.S. Karthik Kumar, Neena Susan Alex, Visual Cryptography Using Hybrid Halftoning, Procedia Engineering, Volume 38, 2012, Pages 2117-2123, ISSN 1877-7058, Retrieved from <http://dx.doi.org/10.1016/j.proeng.2012.06.254>.
4. M. Jenila Vincent, E. Angeline Helena, Securing Multiple Color Secrets Using Visual Cryptography, Procedia Engineering, Volume 38, 2012, Pages 806-812, ISSN 1877-7058, retrieved from http://dx.doi.org/10.1016/j.proeng.2012.06.101
5. Jyoti Jakhar, Pami Dey, M. Dutta, D.K. Bhattacharyya, CellTCS:A Secure Threshold Cryptography Scheme based on Non-linear Hybrid Cellular Automata, Procedia Technology, Volume 6, 2012, Pages 947-953, ISSN 2212-0173 , retrieved from <http://dx.doi.org/10.1016/j.protcy.2012.10.115>.
6. Shouchao Song, Jie Zhang, Xin Liao, Jiao Du, Qiaoyan Wen, A Novel Secure Communication Protocol Combining Steganography and Cryptography, Procedia Engineering, Volume 15, 2011, Pages 2767-2772, ISSN 1877-7058, retrieved from <http://dx.doi.org/10.1016/j.proeng.2011.08.521>.
7. Sandeep Gurung, Mrinaldeep Chakravorty, Abhi Agarwal, M.K. Ghose, Multiple Information Hiding Using Circular Random Grids, Procedia Computer Science, Volume 48, 2015, Pages 65-

72, ISSN 1877-0509, retreived from <http://dx.doi.org/10.1016/j.procs.2015.04.111>.

1. Amitava Nag, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar, A new (k, n) verifiable secret image sharing scheme (VSISS), Egyptian Informatics Journal, Volume 15, Issue 3, November 2014, Pages 201-209, ISSN 1110-8665, Retrieved from <http://dx.doi.org/10.1016/j.eij.2014.10.001>
2. A. Angel Rose, Sabu M. Thampi, A Secure Verifiable Scheme for Secret Image Sharing, Procedia Computer Science, Volume 58, 2015, Pages 140-150, ISSN 1877-0509, Retrieved from <http://dx.doi.org/10.1016/j.procs.2015.08.042>
3. Tapasi Bhattacharjee, Jyoti Prakash Singh, Amitava Nag, A Novel (2,n) Secret Image Sharing Scheme, Procedia Technology, Volume 4, 2012, Pages 619-623, ISSN 2212-0173, Retreived from <http://dx.doi.org/10.1016/j.protcy.2012.05.099>.
4. Feng Liu, Wei Qi Yan, Visual Cryptography for Image Processing and Security: Theory, Methods, and Applications, Springer, 20-Aug-2014
5. Rawat, Danda B., Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, IGI Global, 31-Oct-2013
6. Alexey Vinel, Rashid Mehmood, Marion Berbineau, Cristina Rico Garcia, Chung-Ming Huang, Naveen Chilamkurti, Communication Technologies for Vehicles: 4th International Workshop, Nets4Cars/Nets4Trains 2012, Springer, 23-Apr-2012, Retrieved from <http://link.springer.com/chapter/10.1007%2F978-3-642-29667-3_1>
7. J. P. Weir, Visual Cryptography and Its Applications, Bookboon, 2012
8. Stelvio Cimato, Ching-Nung Yang, Visual Cryptography and Secret Image Sharing, CRC Press, 10-Aug-2011
9. David Salomon, Data Privacy and Security: Encryption and Information Hiding, Springer Science & Business Media, 20-May-2003