Abstract: VANET is an emerging type of distributed network and it is dynamic in nature which provides variety of services such as detecting oncoming collision and provides warning signal to alert the driver. In military application data security is an important issues. This paper presents a secured and an efficient way of sending data and image in encrypted form using HMAC based authentication and Visual Cryptography respectively. Hash based Message Authentication is provided to authenticate node and message digest function MD-1,256,512 are used for message integrity and symmetric key mechanism is carried out in this work. To transmit image securely among the authenticated node, visual cryptography technique is proposed in this paper. Encryption and decryption of image is accomplished by using mathematical algorithm. Digital watermarking scheme with visual cryptography is proposed to secure the confidential image. Image is divided into two images using VCS, it is not possible to recover the original images without accessing both the shares. The OR operator is used to superimpose the two images and fully recover the original template.

Index terms: HMAC, Message Digest Function, Symmetric key, VANET, Visual Cryptography.

1 INTRODUCTION
A. Vehicular Adhoc Network(VANET)
Wireless adhoc network has become one of the prime topics of research in the very recent years where majority of the research work is concentrated on restricted user-groups, where various nodes cooperate to communicate. A Vehicular Ad-Hoc Network or VANET is a form of Mobile Ad-Hoc Network or MANET which provides communication between vehicles and between vehicles and road-side base stations. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network.

Fig 1: A VANET consists of vehicles and road-side base stations that exchange primarily safety messages

Characteristics of VANET which make different from MANETs are
- The position of node changes frequently
- Network size in VANET is geographically unbounded
- The information exchange among node becomes frequent
- VANET is designed for the wireless environment
- The information in VANET must be delivered to the node within time limit
- The VANET nodes have no issue of energy and computation resources [10].

Security and privacy are the two main concerns in designing a VANET [8]. Hence the security requirements for VANETs are
- Authentication
- Message integrity
- Message confidentiality
- Privacy
- Real time guarantees

Although there are many proposed solutions for improving securities in VANET but security still remains an unsolved research subject. The privacy preserving of data or credential is essential in VANET, which is done by complex cryptographic actions. Hence there is necessity of protection of any confidential data while communicated through other nodes or vehicles in VANET.
Since VANET is a distributed network and dynamic in nature, the credential of driver like the license of vehicle, scanned image of passport, any images captured while travelling which is of confidential nature has to be sent to the desired destination. However in order to send this data a suitable privacy preserving of data using some cryptographic actions with less computation time is of highly essential. The phenomenon of privacy preserving guarantees that the vehicle is anonymous and untraceable as well as it also safeguard the driver’s private information during sharing of information with other nodes or vehicles existing in the network. However any attacker can misuse privacy preserving mechanism to provide false information to other vehicles and attempt to reveal any of confidential data that will be transmitting in network[1]. Hence there is a critical need for authentication of vehicle. In this project authentication of vehicle is done by HMAC technology is proposed.

B. Visual Cryptography

Now a day the transmission of data through computer is increasing rapidly. So the security of transmitted data becomes mandatory. Hence VCS is proposed in this paper.

Visual Cryptography Scheme (VCS) is an encryption method used to encode secret written materials. The idea is to convert the written material into a binary image and encode this image into n shadow image, it is also called as shares of images. The decrypting only requires selecting some subset of these n shadow images, making transparencies of them and stacking them on top of each other. Main advantage of this scheme is mathematical computation complexity is reduced compared to conventional cryptographic techniques.

The basic model of Visual Cryptography was introduced by Naor and Shamir in 1994 which accepts binary image I(x, y) as secret image, which is divided into ‘n’ number of shares. Each pixel of image I(x, y) is represented by ‘m’ black and white sub pixels in each of the ‘n’ shared images. It is impossible to get any information about the secret images from individual shares. The other advantage of VCS is that, unlike other cryptography techniques, the secret image recovery does not need difficult computations, i.e the secret information can easily be recovered with enough number of shares through stacking process (human vision) instead of special software or hardware devices.

The various black and white visual cryptography schemes can be summarized as follows:

1) 2 out of 2 scheme: In this, the secret image is distributed on two shares which are both required for the decryption process. This is depicted in figure 3. This scheme can be realized by using either 2 sub pixels or 4 sub pixels to represent each pixel of the secret image as explained below.

a) 2 sub pixels: Each pixel is subdivided into one black and one transparent (white) sub pixel as shown in Table 1

<table>
<thead>
<tr>
<th>Images</th>
<th>White Pixel</th>
<th>Black Pixel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

b) 4 sub pixels: Each pixel is subdivided into four sub pixels, two black and two transparent (white) ones as shown in Table 2

<table>
<thead>
<tr>
<th>Images</th>
<th>White Pixel</th>
<th>Black Pixel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stacking Result</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2) n out of n scheme: In an n out of n scheme the secret message is distributed on n transparencies. Superimposing I transparencies with i < n will not reveal any information of the secret image. There exist two possible ways to construct an n out of n scheme by using 2n sub pixels or 2n-1 sub pixels.

3) k out of n scheme: Splitting of the secret message into n shares out of which any k shares are required for decryption. Contrary to the n out of n scheme, not all n transparencies are required for the decryption in this case k < n [3].

II PROPOSED METHODOLOGY

Implementation of proposed security framework application is always preceded by important decisions regarding selection of the platform, the language used, etc. these decisions are often influenced by several factors such as real environment in which the system works, the speed that is required, the security concerns, and other implementation specific details. Basically the proposed framework is implemented in MatLab a technical computing tool. The proposed framework is modeled using the hash based message authentication, where the two functions or the data is used [1]. The system architecture can be shown in figure 3. The explanation of it is as follows

1. Input Data: The data in the proposed work is the text data.
2. Private Key: The private key is the secret key which will be known by only the source node and the destination node.
3. Hash based MAC value generation: HMAC is used for mutual authentication of nodes. It can use either Message Digest (MD)-1, or of 256 bits,512 bits for hash generation.
4. Authentication of Nodes: The proposed system uses the concept of HMAC to build a security tunnel among two nodes in VANETs. It is as follows, initially using the concept of RSA a token is generated which is pre-distributed among the two nodes which are in need of communication by the Trusted Third Party (TTP). And once the token is distributed among the source and destination node, the role of TTP ends. TTP doesn’t involve in further communication. On receiving the token from TTP the source node uses the token to calculate session key. And using that session key of source node HMAC is calculated at the source node. And destination node also follows the same procedure and calculates its own HMAC.

A HMAC Algorithm

1. Append zeros to the left end of $K$ to create a $b$-bit string $K^*$ (for example, if $K$ is of length 160 bits and $b = 512$, then $K$ will be appended with 44 zero bytes 0x00).
2. XOR (bitwise exclusive OR) $K^*$ with $ipad$ to produce the $b$-bit block $S_i$.

![Fig 3: Proposed Architecture](image)

3. Append $M$ to $S_i$.
4. Apply $H$ to the stream generated in Step3.
5. XOR $K^*$ with $opad$ to produce the $b$-bit block $S_o$.
6. Append the hash result from Step 4 to $S_o$.
7. Apply $H$ to the stream generated in Step 6 and output the result [14].

Now a authentication request message is sent to destination node to source node which consists of the token given by TTP. On receiving the request from source node destination node verifies received token.
with its token. If both the token’s match destination node replies to source node with a reply message which consists of HMAC of destination node. Source node verifies both HMAC’s on receiving the reply message from destination node and if both HMAC’s match replies to destination node by an acknowledgement message. The detailed steps for proposed protocol: Consider a TTP and communication is between node A and node B. And notations used in protocol.

Table 3 Notations used in protocol to communicate between node A and node B

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q</td>
<td>A large prime number.</td>
</tr>
<tr>
<td>AReq</td>
<td>Authentication Request Packet</td>
</tr>
<tr>
<td>BRes</td>
<td>Authentication Response Packet</td>
</tr>
<tr>
<td>F</td>
<td>Point on elliptic curve</td>
</tr>
<tr>
<td>A</td>
<td>Long term secret of node A</td>
</tr>
<tr>
<td>B</td>
<td>Long term secret of node B</td>
</tr>
<tr>
<td>SKAB</td>
<td>Session key generated between node A and B</td>
</tr>
<tr>
<td>SKBA</td>
<td>Session key generated between node B and A</td>
</tr>
</tbody>
</table>

**B Proposed Algorithm for authentication of nodes**

Step 1: TTP calculates the token and distributes it among node A and node B.
Step 2: On receiving token from TTP. Node A selects rA randomly, where 1 ≤ rA ≤ q − 1 and then computes QA = rA.P. And node A sends Authenticated request packet AReq(tokenA, QA).
Step 3: After receiving AReq message, node B first verifies node A’s token. If the A’s token is verified using the B’s token given by TTP.
Step 4: Node B selects randomly an integer rB in the range 1 ≤ rB ≤ q−1 and computes QB = rB · P . It then computes SKBA = H((rB+b) · (QA+PubA)) as a session secret key between A and B.
Step 5: Node B computes HMACB = H(SKBA ||H((QB.x + QA.x)||(QA.y + QB.y))). It then constructs a message m consists of HMACB and QB, that is, m = HMACB||QB and generates a signature sigB (m) on m as sigB (m) = (r,s) using the private long-term key b of B with the help of ECDSA signature generation algorithm. Node B finally sends BRes(m, sign (m)) as an authentication reply message to node A.
Step 6: After receiving BRes message, node A first verifies the signature sigB (m) using the public key of node B with the help of ECDSA signature verification algorithm. Node A then computes SKAB = H((rA+A) · (QB+PubB)) as a session secret key between A and B. And then calculates HMACA = H(SKAB ||H((QB.x + QA.x)||(QA.y + QB.y))).

**Step 7:** Node A compares both HMACA and HMACB for integrity check and if the check holds then as an initiator node A sends an authentication acknowledgement message to node B. In this way both node A and node B use the secret

**C Visual Cryptography Technique**

In the Proposed scheme to transmit an encrypted image (2, 2) Visual Cryptography Scheme is used. The whole design is divided into two process

1) Encryption(Creating shares)
2) Decryption(Human Visual System)

Encryption process

Encryption process is partitioned into two stages and shown in figure 2.

1.First stage

An original binary image of size 261X127 has been considered in this design where each pixel is either 0 or 1. A (2, 2) Visual Sharing technique is applied on original binary image. From this process two binary share images will be generated.

2.Second stage

In the second stage four share images are generated from the two share images obtained from first stage using (2,2) VCS, this is called chain share of order 2.

Decryption process

Decryption process is reverse process of encryption. It consists of two stages and pictorial representation of decryption process is given in figure 2

1.First Stage

From four decrypted share of the previous step, two partial shares were obtained by performing bitwise logical ORing between share 1,2 and share 3,4.

2.Second Stage

Bitwise logical OR operation performed on two obtained share images from previous stage to get back the retrieved image. The obtained image is identical to original image [2].

**Table 2 (2, 2) Visual Cryptography Sharing Scheme**
Table 1

<table>
<thead>
<tr>
<th>Pixel</th>
<th>White</th>
<th>Black</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prab.</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Share 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stack share 1 &amp; 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IV Conclusion

The below figures show simulation results of the proposed work. It is made as user interface where user can enter the number of nodes and the communication range between the nodes and the red color in the figure6.a shows the authenticated nodes and the blue color shows the two nodes in the communication range. Once the nodes are authenticated then the encrypted image is transmitted by source node and at the receiver transmitted image is decrypted. Encryption & decryption is done by using Visual cryptography technique. Original image, encrypted image, decrypted image is shown in the figure 6.

Fig 6.a: Two nodes in the range of communication

Fig 6.b: Authentication of nodes

Fig 6.c Original Image

Fig 6.d Share 1

Fig 6.e Share 2

Fig 6.f Recovered Image

REFERENCES


