Real Time Advanced Data Security Enhancement System with Image Processing

[1] R.Jayapriya, [2] D.Thatshayini, [3] A.Vembu, [4] R.Karthika.
Ponnaiyah Ramajayam College of engineering and technology

Abstract: **Recently, More Peoples they need to implement on TMS Processor using REAL TIME analysis to Data Secret Data hiding (DH) in encrypted images, since it maintains the excellent property that the original cover can be loss less recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this paper, we propose a novel method by reserving room before encryption with a traditional DH using LSB algorithm, and thus it is easy for the data hide to embed data in the encrypted image. The proposed method can achieve real process on TMS, data extraction and image recovery is free of without error. The secrete data which is classified as unknown is sent to the mobile of the owner as a MMS through the operating GSM modem. The owner upon receiving the information commands the system and the fuel is regulated using the relay in accordance with the command of the owner. This would be effective to authenticate the person under different environment and to have an efficient way of security.**

***Keywords*:-LSB, secrete data hiding, encryption, decryption, TMS processor, GSM.**

I. INTRODUCTION

The use of vehicle becomes important everywhere in the world and also preventing it from theft is required. The security features of their products by introducing advanced automated technologies to avoid the thefts particularly in case of image transmission. Since the rise of the Internet, one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have

Been developed to encrypt and decrypt data in order to keep the message Secret.

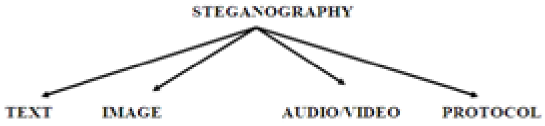

Fig. 1: Different Types Steganography

Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. Steganography is the method of hiding the information about the communication that occurs by hiding information in other information.

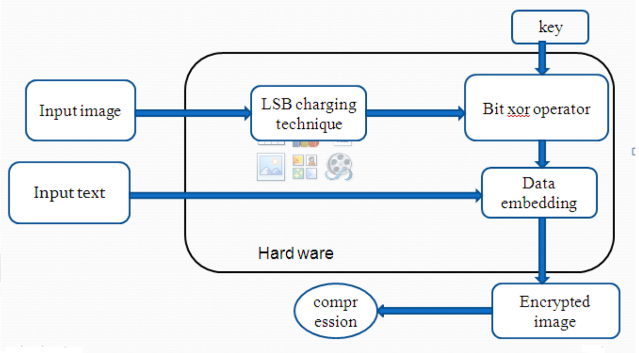

Fig 2Block Diagram: Embedding Process.

It is the art of concealing a message in a shield without leaving a notable track on the original message. It can be pronounced as "ste-g&-'nä-gr&-fe" and derived from Greek words, "Steganos" means "covere" and "Graphie" means writing. Stenography is ancient art and its origins can be located back to 440 BC. The Greek historian Herodotus writes of a nobleman, Hostages, who used steganography for the first time in history. In security system, the objective is to prevent the theft and ensure safety of hackers by avoiding the means of theft.

The goal of Steganography is to conceal the whole segments of communication making the true message not detectable to the observer.

Although Steganography resembles Cryptography and its applications in some aspects, many principal differences exist. Cryptography is about disguising the whole sections of the message whereas the encrypted data package is itself evidence of the existence of valuable information. Steganography acts in advance and makes the encrypted text invisible to illegitimate users. Watermarking and finger printing are two other technologies that are closely related to Steganography; both of them associatedwith safeguarding of intellectual property. But Steganography is associated with hiding of text in the form of information such as image, text, audio, and video.

A. Image

An image can be defined as a two-dimensional signal (analog or digital), that contains intensity (grayscale), or color information arranged along an x and y spatial axis.An image is alsoa collection of pixels, and each pixel has a particular color; thatcolor is described by the amount of red, green and blue in it.

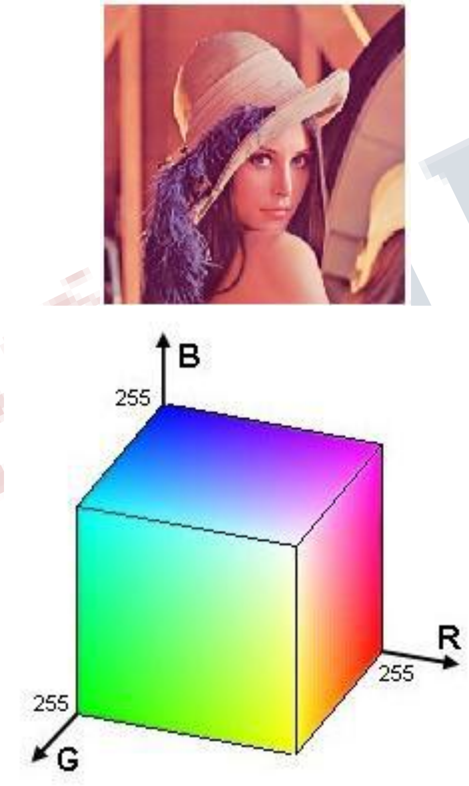

Fig 3: Input Image of Color Component

If each of these components has a range 0–255, this gives a total of 2563 different possible colors. Such an image is a "stack" of three matrices; representing the red, green andbluevalues for each pixel.This implies that every pixel corresponds to 3 values.

B. Secret Data Process

With the help of chaos algorithm our secret data would beconverted to ASCII Format.

Eg.:**JAYA PRIYA**

Encrypted data: @#*&$

C. Image Encryption

The original image in uncompressed design and each pixel with gray value coming under[0,255], denoted by 8 bits. In encryption stage, the XOR results of the original bits and pseudo-random bits are calculated. Chaos is a symmetric key algorithm which is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table.

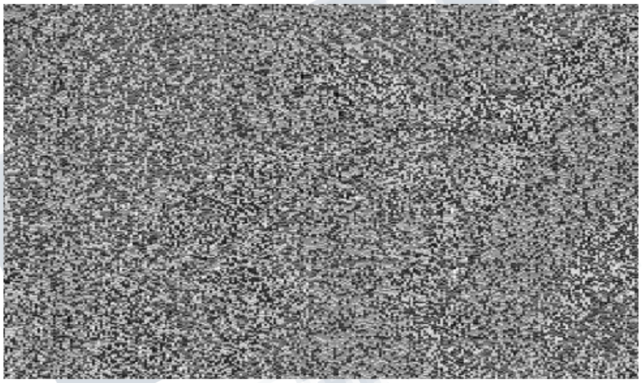

Fig 4.encrypted images

The state table is used for generation of pseudo-random bits and thensubsequentlygenerates a pseudo-random stream which is XORed with the plaintext to give the cipher text.

(a).Pixel processing

In the data embedding stage, some parameters are embedded into a small number of encrypted pixels and the LSB of the other encrypted pixel are compressed to create a space for inserting additional data and the original data at the location occupied by the parameters.

The matrix of a gray scale image of 8 bit consists of m × n pixels and a hidden message consisting of k bits.The first bit of message is embedded into the LSB of the first pixel of first bit and the second bit of message is embedded into the first pixel of second bit for Reversible Manner of secret data selection. The Stego-image generated that holds encrypted message also of 8-bit and difference between the cover image and the above is not visually detectable.

C) Data Extraction and Image Recovery

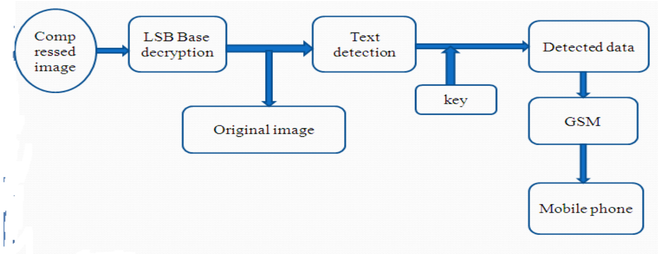

Fig 5: Block Diagram: Extracting Process

It is important to recognize that payload location only reveals the message bits, not the message itself. In order to obtain the message, we must arrange the located payload in their logical order of encrypted images, the cloud server scores the images by embedding some notation, including the identity of the owner of the image, cloud server and time stamps, to handlethe encrypted images. In this stage, the three cases are taken into account that a receiver has only the data-hiding key, only encryption key, and both the data hiding and encryption keys, respectively.

D.Secrete of Data Hide in encrypted recovered Image

The primary reason why payload location fails to establish this order is due to the fact that it assumes each STEGO image carries a fixed payload of size m. By relaxing this constraint the size of each payload can vary between 1 and m. In such case, we show that the mean residuals possesssufficient information to logically order the established payload to recover the encrypted image.

Fig 6: recovered image

The next two sub-sections establish this fundamental result for simple Steganography and group-parity Steganography, respectively

II. TMS PROCESSOR

Digital Signal Processing encompasses a variety of applications, such as digital filtering, speech and audio processing, image and video processing, and control. All DSP applications share some• DSP techniques are under constant development. This implies that DSP systems should be flexible to support changes and improvements in the state of the art. As a result, programmable processors have been the preferred way of implementation. In recent times, though, fixed-function devices have also been introduced to address high-volume consumer applications.

III. GSM:-

GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers. The GSM network is divided into three major systems: the switching system (SS), the base station system (BSS), and the operation and support system (OSS).

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves.

IV. SMS:

SMS is an area where the modem can be used to provide features like: •Pre-stored SMS transmission

- These SMS can be transmitted on certain trigger events in an automation system
- SMS can also be used in areas where small text information has to be sent. The transmitter can be an automation system or machines like vending machines, collection machines or applications like positioning systems whereThe navigator keeps on sending SMS at particular time intervals. SMS can be a solution where GSM data call or GPRS services are not available.
- When the image processing classifier is the secrete data is send through the sms using GSM modem.

V. RESULT AND DISCUSSION:-

The data hiding key can be used to decrypt the planes and additional data would be extracted by directly reading the decrypted version. The information over encrypted images can be updated after replacing of lsb and again encrypts the resulted updated information according to the data hiding key. The whole process is leakage proof as it is entirely conducted on encrypted domain. On the other hand, if the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such bank, ATM, defence, secure communication.

VI. CONCLUSION:-

In this paper, an embedded automotive security system involving face recognition is presented. The system can be used to reduce the increased vehicle theft and allows the owner to identify the intruder thereby having the vehicle under his/her control. The results obtained through the face recognition shows that it can be relied upon to ensure safety of vehicle. The system is also reliable to be used in other authorization applications involving robotics, border management, banking security involving ATMs.

REFERENCES

[1] S. Janakiraman, “Pixel Bit Manipulation for Encoded Hiding-An Inherentstego,”*IEEE*, vol. 978, pp. 1-4577, 2012.

[2]B. Schneier, “Applied Cryptography Protocols, Algorithm and Source Code in C,”2nd ed. *Wiley India edit*ion, 2007.

[3] W. Zhang, B. Chen, and N. Yu, “Capacity-approaching codes for reversible data hiding,” Proc 13th Information Hiding(IH’2011),LNCS, vol. 6958, pp. 255–269, Springer-Verlag, 2011.

[4] A. Cheddad, J. Condell, K. Curran and P. Mc. Kevitt“Digital Image Steganography:Survey and Analysis of Current Methods,”

[5] W. Zhang, B. Chen, and N. Yu, “Improving various reversible datahiding schemes via optimal codes for binary covers,” *IEEE Trans.Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[6] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” *IEEE Trans.Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.

[7] P. Tsai, Y. C. Hu, and H. L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Process., vol. 89, pp. 1129–1143, 2009.

[8] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[9] X. Zhang, “Reversible data hiding in encrypted images,” *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[10] W. Hong, T. Chen, and H.Wu, “An improved reversible data hiding in encrypted images using side match,” *IEEE Signal* Process. *Lett.*,vol. 19, no. 4, pp. 199–202, Apr. 2012.