Securing Criminal Records using R-Pi, QR code and Steganography

Asha Durafe

Abstract*: *In today`s digital scenario it has become very essential to maintain secrecy of criminal records otherwise forgery could happen. Using steganography it is possible to provide security for the information which is communicated over the internet from one crime branch to the other. Steganography one of the emerging security fields works to mask the very existence of the message. A wide range of carrier file formats can be utilized, but digital steganography is the extremely beneficial data hiding technique to secure criminal image as well as the crime scene images. Various applications have various prerequisites of the steganography method utilized. In this paper, we proposed CRSS (Criminal Record Security System) an image steganography method with LSB and RSA technique for enhanced security and along with that Raspberry pi and GSM module is used. Thus, for a more secure approach, the proposed method hides the criminal`s confidential records such as criminal`s image, crime scene digital images etc. using LSB steganography and also encrypts the confidential data making use of a private key using RSA algorithm and then sends it to the desired end. The receiver then decrypts the confidential data to get the original criminal information. CRSS is also proposed to send a QR code to the receiver which hides sensitive data and may include criminal`s previous crime history and other written proofs which are scanned at the receiving end reveals the entire criminal record. The entire system is implemented on Raspberry Pi 3 processor and thus a secure transmission of data without traditional desktop dependency in a more economical way could be established.

Keywords*: *Steganography, Data Hiding, Least Significant Bit (LSB), RSA, Raspberry-Pi, QR code, GSM.

I. INTRODUCTION

Hiding confidential data inside images has become a well-accepted method in today`s cyber world. An image with a secret confidential data inside can easily be spread across the cyber world or in digital media. The use of steganography in digital media has been explored by German steganographic expert Niels Provos, who researched a scanning cluster which probes the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited [1]. Image Steganography is the method of concealing the information within the image so as to prevent the unintended user from the detection of the confidential messages or data.

To conceal the confidential data inside an image without losing its visible properties, the cover image can be adjusted in noisy areas with a good amount of color variations, so less attention will be emphasized towards the alterations [1]. The most common technique to make these modifications involves the utilization of the Least Significant Bit or LSB, masking, filtering and transformations on the cover source [2]. The technique may be implemented using diversified acquisition levels on various formats of image files. Image steganography deals with concealing confidential data i.e. text, images, audio or video files in another text, image, audio or video files. The proposed strategy plans to utilize steganography for an image with another image using spatial domain technique. This confidential criminal image can be reconstructed solely through correct decoding system. This hiding and retrieval of the images is done using MATLAB codes on Raspberry Pi 3 where traditional desktop interface is not mandatory and a GSM interface is used to send the secret key. A QR code scanner at the receiver crime branch is used to retrieve the confidential data through a QR code sent from the sender crime branch.

Steganography focuses on concealing the confidential data in a cover image in such a manner that unauthorized users are unable to identify the existence of confidential data by just detecting the information. In contrast to watermarking, steganography does not intend to prevent the hidden information by opponents of removing or changing the hidden message, which is hidden in the cover image but it ensures that it remains unnoticeable. Steganography is of particular interest in systems wherein encryption cannot be utilized to secure the communication of secret information.

II. STEGANOGRAPHY VS. CRYPTOGRAPHY

Cryptography is the art of encrypting data in such a way that one cannot make sense of the encrypted message, whereas in steganography the mere existence of data is masked in a way that even its occupancy cannot be detected. Using cryptography might raise some suspicion whereas in steganography the existence of the confidential message is imperceptible and thus not detectable. We can think of steganography as an added layer of security in cryptography, and it is generally advisable to use where just encryption is not sufficient.

III. STEGANOGRAPHY WITH LEAST SIGNIFICANT BIT (LSB) METHOD

Since many years steganography is the technique used for transferring information in a way which conceals the mere presence of the confidential data. Steganography plays a vital role in information security.

Revised Manuscript Received on April 1, 2020.
***** Correspondence Author
Asha Durafe, Department of Electronics Engineering, Shah & Anchor Kutchhi Engineering College, Mumbai. . Email: asha.durafe@sakec.ac.in

It is the art of invisible communication by concealing confidential data inside cover information [3]. The word steganography is originated from Greek which exactly means concealed writing. An Image Steganography technique involves three major components: cover image (which hides the secret image), the secret image and the stego-image (which is the cover image with secret image embedded inside it). A digital image is always mode led using a 2-D matrix of the color model at each grid point (i.e. pixel). Generally, gray images use 8 bits and colored images use 24 bits to outline the color model known as RGB model. The Image Steganography technique which utilizes an image as the cover, there are numerous methods to hide confidential data inside cover image. The spatial domain methods adjust the cover-image pixel bit values to conceal the secret data. The secret bits are composed legitimately to the spread cover image pixel bytes. That being so the spatial domain techniques are uncomplicated and simple to put into practice. The Least Significant Bit (LSB) steganography is amongst the majorly used techniques in spatial domain techniques. The idea of LSB Embedding is simple. It probes into the fact that the degree of precision in various image formats is far more noteworthy than that noticeable by normal human vision. Accordingly the modified image with slight changes in its hues will indistinct from the original by an individual, just by taking a gander at it [4].

IV. SECURITY OF SECRET DATA

In view of abstaining from the increasing intuitions of eavesdroppers, while escaping from the extensive screening of algorithmic detection, the confidential data must be unnoticeable both intuitively and statistically. A highly imperceptible Stego-image should be resulted by the Steganography techniques.

V. PAYLOAD SIZE

Apart from watermarking technique which is intended to integrate only a small amount of confidential information, steganography focuses at hidden communication and hence it generally demands good amount of embedding capacity [5]. Requirements for large payload and secure communication are often clashing. On the grounds of the various application frameworks, a trade-off between payload and security should be met.

VI. ROBUSTNESS

It is prime important to provide robustness to Stego-image due to the image processing techniques like compression, cropping, resizing etc. It means when any of the mentioned techniques are applied on stego image, hidden data must not be impaired completely. There is no technique of steganography which provides all the three properties at a peak level. There is a trade-off between the payload capacity and the robustness to certain attacks, while keeping the perceptual quality of the stego image satisfactory level.

VII. PROCESS FLOW OF PROPOSED ALGORITHM

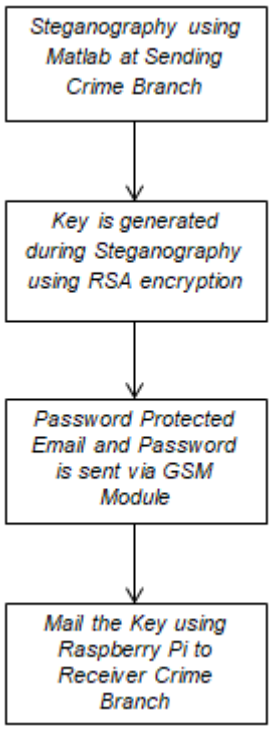

Fig. 1 Transmission process

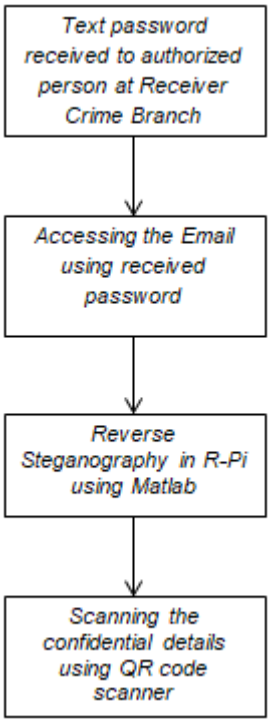

Fig. 2 Reception process

There are two elements with which information will be transferred by the given process as shown in fig. 1, one is the image and other is the data. The image of a criminal will undergo Steganography process and criminal`s confidential data and other evidence will be transferred using QR code which will be scanned by the receiver upon receiving the data. Transmission Process:

Step 1: First process is Steganography. A Cover image is selected first, followed by a secret image that is smaller in size compared to the cover image. Then the process of LSB Steganography is performed in MATLAB.

Step 2: After Steganography is completed, a private key using RSA encryption is generated which is essential in the receiver end without which the inverse Steganography isn't possible.

Step 3: After completion of Steganography and key generation, Email will be sent to the receiver consisting of stego-image and private key as QR barcodes which are protected by passwords.

Step 4: These passwords are sent via text message (SMS) using the GSM module SIM800L.

Extraction Process:

Step 5: On receiving the mail as shown in fig. 2, the user will scan the QR Barcodes to get the secret image and the data related to the secret image.

Step 6: The data is received, but the image received is stego-image which needs to be decrypted using inverse Steganography.

Step 7: The private key generated while Steganography process and transmitted via mail, is used to process the inverse Steganography so as to view the original secret image.

VIII. FUNCTIONAL REQUIREMENTS

Useful necessities are the prerequisites that define specific conduct or capacity of the framework.

- Login: This function will validate the sender if username and password are accurate else it will exit the system.
- Secret Image: This will be the secret criminal image which is to be hidden.
- Cover Image: Cover Image is the image to be selected in which secret criminal image can be hidden.
- Stego Image: Encryption and LSB implementation is performed on cover image to hide secret criminal image by replacing bits of cover image by the bits of criminal image.
- Sender: in this Sender sends this stego image file to the intended receiver to which he does want to establish communication.
- Receiver: The receiver accepts the stego image and with the help of RSA secret key after decryption reconstruction algorithm is applied to retrieve the secret criminal image.

IX. NON-FUNCTIONAL REQUIREMENTS

- Safety Requirements: Sender and Receiver should make sure that only they are having the accurate algorithms to encrypt and decrypt the secret image inside cover image. Sender and Receiver should refrain from eavesdropping.
- Security Requirements: The proposed method describes an algorithm in which embedding secret image in cover image is discussed. Only sender and receiver should be aware of encrypted files. Users should not unfold the message regarding sent images and also the receiver information.
- Software Quality Attributes: The Quality of the algorithm is supported with crucial security such that only sender and receiver can communicate through image. There is no likelihood of finding a secret image.

A. Hardware requirement

The hardware used in this system is really basic and replaceable. The hardware used in this project is:

1. QR scanner
2. GSM Module- GSM 800L
3. Raspberry Pi 3

B. The Encoding Process

The steganography technique used is LSB coding.

Step 1: The offset of the cover image is recovered from its header.

Step 2: That offset is left as it is to maintain the respectability of the header, and from the following byte, we start our encoding procedure.

Step 3: For embedding, we first take the input cover image which is a RGB image file and then instruct the user towards the selection of the secret Image file for hiding.

Step 4: The secret image file is taken as input and divided in stream of bytes.

Now, each bit of these bytes is encoded in the LSB of each cover image pixel.

Step 5: At the end of the encoding process we get the stego image that contains the encoded secret Image and it is saved, at the specified path given by user, in JPG format using this method. This finishes the embedding process.

C. The Decoding Process

Step 1: The offset of the image is recovered from its header.

Step 2: Allot the user space using the same procedure as in the embedding process.

Step 3: Using LSB method the data of the image is stored into byte array.

Step 4: Using the above byte array, the bit stream of the original output image file is stored into another byte array. And the above byte array is written into the decoded image file, which leads to the original criminal image.

These common weak points of traditional LSB steganography are the sample value changes asymmetrically. The proposed algorithm overcomes this problem as the image is stored as a separated stream of bytes. In this method LSB with pseudo random generator is implemented. The pseudo-random number generator is implemented for this cause and its seed is taken as key of steganography along with RSA key. First of all an array of random numbers, with the length equal to secret bit-stream, is generated using key. By using this array, the number of pixel positions is calculated. Now secret bits are embedded in the LSB of these pixels.

X. RESULTS AND DISCUSSION

A. Open cover image:

This is the image of the Matlab GUI of the developed steganography system. This frame prompts you to upload the cover image to hide secret criminal image.

B. Open secret image:

This frame prompts you to input the secret image of criminal which is to be hidden inside the cover image and at the same time secret keys using RSA are generated.

Fig. 3 Opening the cover image

C. Steganography:

It is claimed as a one-way function of converting plain image into cipher image or concealing secret image into plain image and it can be reconstructed only with the knowledge of secret keys.

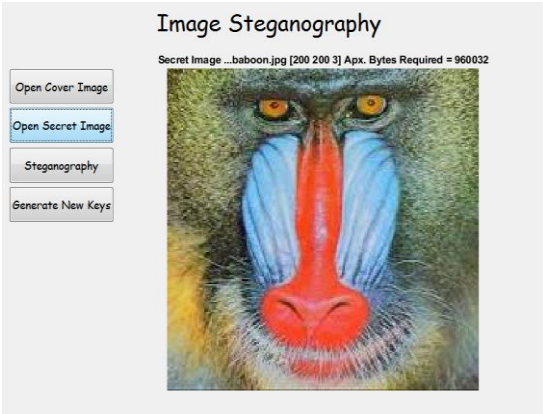

Fig. 4 Opening the secret image

D. Generate new key:

The multifaceted design of finding a private key from a RSA open key closely resembles figuring the modulus n. An aggressor in this manner can't utilize information on a RSA open key to decide a RSA private key except if he can factor n. It is likewise a single direction work going from p q esteems to modulus n is simple yet invert is unimaginable.

On the off chance that both of these two capacities are demonstrated non single direction, at that point RSA will be broken. Indeed, on the off chance that a system for figuring proficiently is grown, at that point RSA will never again be sheltered. The quality of RSA encryption definitely goes down against assaults if the number p and q are not huge primes as well as picked public key e is a modest number.

When the key pair has been created, the procedure of encryption and decoding are generally direct and computationally simple. Strangely, RSA doesn't legitimately work on series of bits as in the event of symmetric key encryption. It works on numbers modulo n. Subsequently, it is important to speak to the plaintext as a progression of numbers not as much as n.

Considering that an eavesdropper intercepts the embedded image and wants to decode it. Obviously he additionally approaches the public key. What he doesn't have is the private key and in different words he should factorize the extremely huge whole number n into the prime components p and q. However, this is troublesome in the current situation with Mathematics: there are no realized calculations to do this in a worthy time.

E. Private Key:

Every recipient has a special unscrambling key, by and large alluded to as his private key. Private and public keys are connected numerically; it isn't attainable to figure the private key from the public key. Truth to be told, the savvy some portion of any public key cryptosystem is in structuring a connection between two keys. The Main focal points of this framework are: it gives security to the confidential data without knowing to the unintended receiver, Number of bits been supplanted by client or sender along these lines the unintended receiver can't figure secret key, Normal system client can't figure secret image.

Fig. 5 Generation of secret key

F. The Hardware Platform

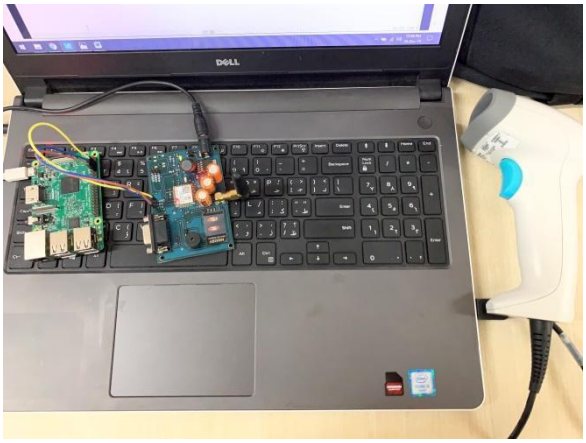

Fig. 6 Raspberry Pi 3, GSM Module and QR code scanner

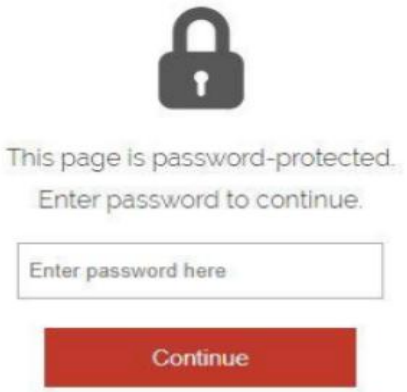

Fig. 7 Entering the authorized password

Fig. 8 QR Code

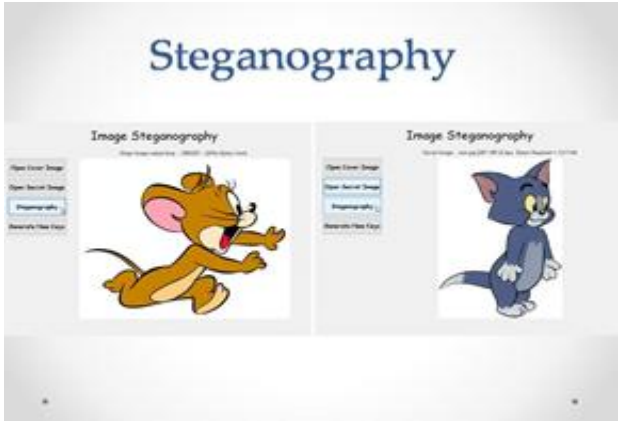

Fig. 9 Steganography

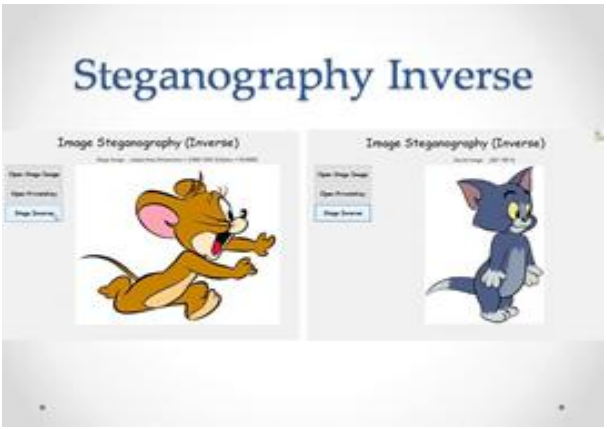

Fig. 10 Inverse Steganography

XI. PERFORMANCE ANALYSIS

A. MSE: Mean Square Error is one of the measures used to verify the quality of images and measures the difference between the intensities of secret image and extracted image. Mathematically it can be expressed as,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}((f(i,j) - f'(i,j)) * (f(i,j) - f'(i,j)))$$

*f(i,j)*is the secret image and *f'(i,j)* is the extracted image. Lower value of MSE is always desired.

B. PSNR: Peak Signal to Noise Ratio is another statistical measure used to evaluate the difference between secret image and extracted image. Mathematically PSNR is,

$$PSNR(dB) = 10\log(\frac{255*255}{MSE})$$

Higher value of PSNR is always desired [16].

Table- I: PSNR and MSE values

Cover Image	Secret Image	MSE	PSNR
Lena	Baboon	1.014	50.13
Tom	Jerry	1.106	49.61
Pepper	Cameraman	1.153	47.35
Boy	Moon	1.461	46.03

XII. CONCLUSION

In most of the proposals on Criminal Security Systems it is observed that they offer good amount of security attributes. However, many of them are dependent on costly processors for their execution. A novel data hiding security system is generated named CRSS with the combination of minimal hardware and software to hide the confidential records of criminals which can be used by the Police Department Crime Branch.

The criminal data might be changed for deceiving the police office. The information that can be changed or altered is mostly the kind of wrongdoing performed, which can be changed for lessening the discipline of the guilty party. The proposed framework gives security to criminal information from unapproved access and altering. The same method can be used for different applications like medical imaging security, social media security, protection against internet data tampering and many more. Due to LSB encoding it has high payload capacity with encryption advantages of RSA algorithm which intensify the security attributes.

REFERENCES

1. Masoud Nosrati, Ronak Karimi, Mehdi Hariri, An introduction to steganography methods, World Applied Programming, Vol (1), No (3), August 2011,pp. 191-195.
2. Imran Khan, Bhupendra Verma, Identifying covert message inside a steganographic image using Neural Network, Proceedings of the International Conf. Computer and Network Technology, 2009, pp. 149-153.
3. Vikas S. Kait, Bina Chauhan, BPCS steganography for data security using FPGA implementation, International Conference on Communications and Signal Processing (ICCSP), 2015, pp. 1887-1891.
4. Patidar V, Purohit G, and Pareek NK. 2017. A Novel Quasigroup Substitution Scheme for Chaos Based Image Encryption. J. Applied Nonlinear Dynamics, Vol. 7, pp. 1-33.
5. Leo Lee, LSB Steganography:Information Within Information, Computer Science 265, Section 2, Professor Stamp, April 5, 2004, pp. 1-7.
6. Tamanna, Ashwani Sethi,International Journal of Computer Applications Volume 170 – No.8, July 2017, pp. 0975 – 8887
7. Cheddad A, Joan C, Kevin C, Paul M. 2009. Digital Image Steganography: Survey and Analysis of Current Methods. Int. Journal of Signal Processing. Vol. 90, pp. 727-752.
8. Hussain M, Ainuddin WB, Abdul W, Mohd Yamani IBI, Anthony TS. HO, Ki-Hyun J, Image Steganography in Spatial Domain: A Survey. J. Signal Processing: Image Communication, Vol.65, 2018, pp. 46-66.
9. Kamaldeep J, Gill S, and Yadav R, A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the GrayScale Image. J. Comp. Netw. and Communic, 2018, 9475142:1-9475142:10.
10. Lifang Y, Yao Z, Rongrong N and Ting L. 2010. Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm. Eurasip J. Advances in Signal Processing, 2010:876946.
11. Ratnakirti R, Changder S, Sarkar A, Narayan CD, Evaluating Image Steganography Techniques: Future Research Challenges. Proc. Intl. Conf. Comp. Mgmt Telecomm. Vietnam, Jan. 21-24 2013, pp. 309-314.
12. Sabry S. Nassar NM, Ayad,HM, Kelash HS, El-sayed,MA. M. El-Bendary,Fathi E. Abd El-Samie, Osama SF, Secure Wireless Image Communication Using LSB Steganography and Chaotic Baker Ciphering. Wireless Personal Communications, Vol. 91, 2016, pp. 1023–1049.
13. Asha Durafe, A Review of Digital Steganography Methods, Intl. Journal of Creative Research and Thoughts, Vol.5(4), 2017, pp.1129-1134.
14. Patidar, V., Pareek, N. K., Purohit, G. & Sud, K. K. [2011] "A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption," Optics Communications 284, 4331-4339.
15. Shannon, C. E. [1949] "Communication theory of secrecy systems," Bell System Technical Journal 28, 656-715.
16. Nassar, Sabry S. Ayad, Nabil M.Kelash, Hamdy M.El-sayed, Hala S.El-Bendary, Mohsen A.M.Abd El-Samie, Fathi E.Faragallah, Osama S.Secure Wireless Image Communication Using LSB Steganography and Chaotic Baker Ciphering, Intl. Journal of Wireless Personel communications, 2016, pp.1024-1049
17. Xin Zhou, Xiofei Tang, Research and Implementation of RSA algorithm for encryption and decryption, Proceedings of 2011 6th International Forum on Strategic Technology, IEEE, 2011, pp. 1118-1121.

AUTHORS PROFILE

Asha Durafe has done her B. E. in Electronics Engineering in 2003. Then she has completed M. Tech. in Electronics Engineering from V.J.T.I. Mumbai in 2011. Currently she is pursuing Ph.D. in Electronics and Communication Department of Sir Padampat Singhania University, Rajasthan, India. She is also working as Assistant Professor in Electronics Engineering Department of Shah & Anchor Engineering College, Mumbai, India. Her areas of interests are cyber security, Digital Image Processing, Computer Networks, Advanced Networking Technologies and IPR and Patenting.