Design and Implementation of Secured Data Embedding Method using Quick-Response Code and COLOR LSB

[1]J.N.V.R.Swarup Kumar, [2]Mannem Sailaja

[1,2]Department of CSE, Gudlavalleru Engineering College, India.
Email: [1]swarupjnvr@yahoo.co.in

Abstract : Steganography is the study of concealing the reality in the data which we are sending. The objective of steganography is to implant a mystery message inside a bit of unsusceptible data. The consequence of steganography relies on upon the mystery of the cover carrier. After the steganographic bearer is uncovered, the security relies on upon the strength of the algorithm and the cryptographic routines utilized. In place, to accomplish secrecy, either the transporter must be made more strong against steganalysis or new and better transporters must be found. The primary aim behind this paper is to examine another steganography procedure for images. Before implanting the secret message, it ought to be encoded utilizing Quick - Response code. The bits from the resultant scrambled message will be covered up inside of the image using COLOR LSB.

Keywords: **Steganography, Cryptography, Segmentation, COLORLSB, Indexed Image, Steganalysis.**

I. INTRODUCTION

Steganography means secured or concealed composition [1, 3]. The objective of steganography is to communicate something specific through a few unsuspicious transporter. The message can be a content, a picture or it can be a sound document. Steganography method helps secluded from everything the way that a mystery message is being sent in unique data. Computerized steganography is an innovation utilized for changing the advanced transporters, for example, pictures or sounds. These progressions are made to conceal the mystery message, yet the successful results ought not influence the transporter.

Steganography systems consolidate numerous parts of computerized sign handling, cryptography, measurable correspondence hypothesis and human recognition. Cryptography is not like steganography. Cryptographic strategies are utilized to scramble a message so that it can't be perused by a third party, the aggressor. In the event that at all a cryptographic message is found, it is troublesome or difficult to comprehend and de-code it, since the message is encoded in human ambiguous format. Steganography shrouds the very presence of a message in the spread medium. It is a decent practice to encode a message utilizing cryptography and after that concealing the encoded message utilizing steganography. The subsequent stego-picture can be transmitted without uncovering that the mystery data has been traded. Besides, if an aggressor were to annihilation the steganographic method and distinguish the message from the stego-picture, he would at present require the cryptographic translating key to unravel the encoded message.

Division is the system of allotting an automated picture into various parts. Using division, we can rework and/or change the representation of a photo into something that is more critical and easier to analyze. Picture division is typically used to consider needed bit of the photo. More totally, picture division is the method of doling out an imprint to every pixel in a photo where the pixels with same name give certain visual qualities.

1. BACKGROUND THEORY

In the most recent few years, the hypothetical establishments of data stowing away has progressed quickly. Displaying the data concealing process as one of the secured correspondences enhanced data concealing calculations and precise models of the channel limit and lapse rates. In the meantime, steganography security, i.e. the capacity of data covering up to serve in a situation where a foe unequivocally goes for invalidating the concealed data objectives, whatever they are, has been perceived as one of the principle open issues in actualizing this method.

As clarified in reference [10], for all the steganographic frameworks, most fundamental and basic necessity is the imperceptibility. The concealed message ought not be distinguished by other individuals. Besides, the spread message with shrouded message i.e. stego-media is undefined from the first ones i.e. spread media. The spread media and stego-media ought to seem indistinguishable under all conceivable measurable assaults and then the implanting methodology ought not debase the media constancy. [8] Presents a few assaults on spread media. The contrast between stego-media and the spread media ought to be impalpable for visual assaults.

Steganography utilizes two sorts of conventions: private key and public key steganography. In private key steganographic model, both sender and recipient impart a secret key before passing on messages. The data message may be in any computerized structure and be dealt with as a bit stream. Open key cryptography obliges the utilization of two keys, one private and one public key. General society key is utilized as a part of the implanting procedure while the private key is utilized as a part of separating the shrouded message.

Eventhough an impressive number of steganographic systems were being used, investigation of this subject in the logical writing retreats to Simmons[5], who in 1983 detailed it as the "detainees' issue". A definite survey on steganographic methods is examined by the creator in her past paper Ref. [2].

2.1 Digital Steganography Methods

The steganography applications range from those that really shroud information, regularly scrambled, inside the document, to those that basically connect shrouded data to the end of a record, for example, Camouflage. As clarified in Ref. [7], the group is concerned with various computerized innovations, to be specific, content records, pictures, films and sound. One of the fundamental techniques normally utilized for steganography includes the methodology of concealing a message in picture pixels. Advanced pictures are the most far reaching transporter medium utilized [9]. Neil F. Johnson [6] clarifies diverse routines for concealing information in computerized pictures.

2.2 Image-based Steganography

The steganography applications range from those that really shroud information, frequently encoded, inside the record, to those that just connect shrouded data to the end of a document, for example, Camouflage. As clarified in Ref. [7], the group is concerned with various advanced advancements, specifically, content records, pictures, films and sound. One of the fundamental systems regularly utilized for steganography includes the procedure of concealing a message in image pixels. Computerized image are the most broad bearer medium utilized [9]. Neil F. Johnson [6] clarifies distinctive techniques for concealing information in computerized images.

Numerous steganographic devices are accessible in the web for shifted image positions. The way that pictures can be subjected to lossy pressure strategies has proposed that additional data could be covered in them. Properties of images including glow, complexity and hues can be controlled. A 24-bit shading image has three segments comparing to Red, Green and Blue. The three parts are ordinarily quantized utilizing 8 bits. A picture produced using these segments is depicted as a 24-bit shading image. Every byte can have a worth from 0 to 255 speaking to the force of the shading. The darkest shading worth is 0 i.e; dark and the brightest is 255 i.e.white. Straightforwardness is controlled by the expansion of data to every component of the pixel information. A 24-bit pixel worth can be put away in 32 bits. The additional 8 bits are utilized for indicating straightforwardness. This is some of the time called the alpha channel. A perfect 8-bit alpha channel can bolster straightforwardness levels from 0 (totally straightforward) to 255 (totally obscure). It can be put away as a component of the pixel information. Current techniques for embedding messages into image carriers fall into three categories [4][7]:

- Least-Significant Bit embedding (or simple embedding)
- Transform techniques.
- Perceptual masking & Filtering Techniques.

2. THE PROPOSED METHOD

This technique uses filed (24 bits/pixel) bitmaps, for example, BMP, GIF & PNG as the bearer medium to conceal mystery writings. Before concealing a mystery message, it ought to be encoded. The bits of mystery message will be covered up inside the chose section of ordered image. High secured applications are come about by utilizing both steganography and cryptography procedures. In an ordered shading image, content is put away in the RGB (red, green, blue) segments of the pixel of the chose fragment. This fragment contains entire message installed as a character every pixel.

There are a few standard LSB strategies: Single-LSB, twofold LSB and so on. For the new procedure, shading LSB is utilized. BMP, GIF and PNG are some ordered picture positions. This new LSB system can be utilized with all the sorts of shading pictures. As the shading LSB permits implanting an entire character into a solitary pixel, more information can be installed in the picture portion.

By utilizing segmentation, the steganography methodology can be made more secure against steganalysis. since it is more hard to distinguish the piece of the picture where genuine content is installed.

COLOR LSB is the procedure of utilizing the RGB parts of a pixel in color image. In this method, an 8-bit character is partitioned into three sections (three LSB bits of the character as first part, next three LSB bits as second part, remaining two MSBs as third part). First and foremost part is installed into the three LSBs of red segment, second part into the three LSBs of green lastly the third part into the two LSBs of blue part.

This bit of work talks about around an instrument that won't just chip away at 24 bit filed color images additionally have the capacity to encode the mystery content utilizing deviated key cryptography and conceal secret instant messages inside the QR image.

The systems utilized for the proposed technique is clarified in the accompanying steps:

3.1 Quick - Response Code

Data encryption is done by following steps:

A QR code embodies dim modules (square spots) organized in a square system on a white establishment, which can be scrutinized by an imaging device, (for instance, a cam) and arranged using Reed–Solomon lapse revision until the picture can be suitably deciphered. The obliged data are then expelled from samples display in both level and vertical parts of the picture.

The mask patterns are characterized on a framework that is rehashed as important to cover the entire image. Modules comparing to the dim territories of the cover are reversed. The organization data is shielded from errors with a BCH code, and two complete duplicates are incorporated in every QR symbol.

The message dataset is put from right to left in a crisscross pattern, as demonstrated as follows. In bigger symbols, this is muddled by the vicinity of the arrangement examples and the utilization of numerous interleaved error-correction blocks.

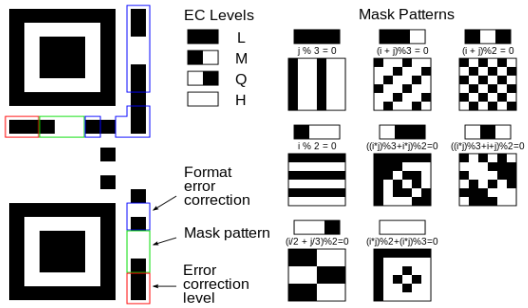

Figure 1: Meaning of design information

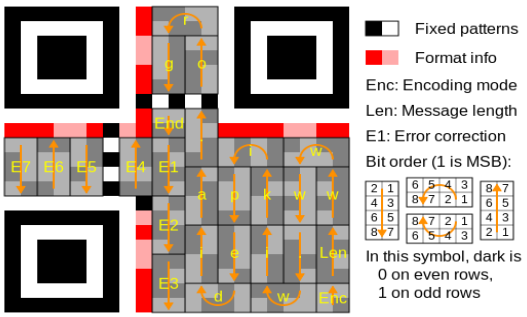

Figure 2: data position within a QR symbol

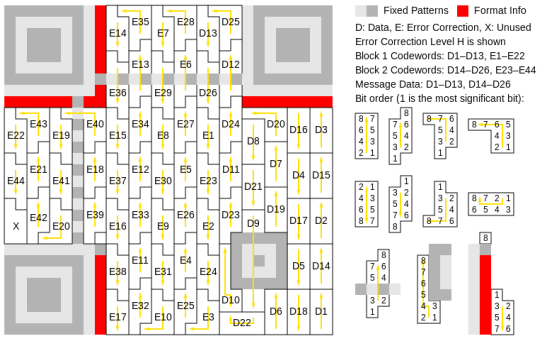

Figure 3: Larger symbol illustrating interleaved blocks

3.2 Hiding Message in the QR Image

The following are required for hiding a message:

1. A carrier image (color)
2. Secret message in text format
3. Quick Response code.

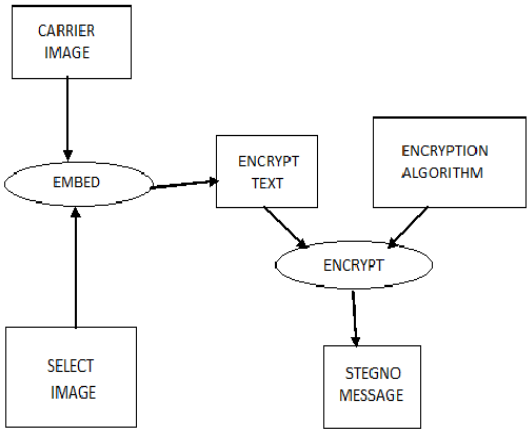

Fig 4: Hiding Message in the Segment

Secret message to be concealed ought to be in content arrangement. Quick Response code is utilized for scrambling the secret message. The quantity of bits in the image ought to be sufficiently sufficient to shroud the scrambled message(QR image). In the event that the measure of information to be covered up is vast, the picture size ought to additionally be expansive. The Stego image utilized for concealing and removing must be same. Distinctive QR images can be utilized for diverse messages. Figure1 above shows the procedure of message stowing away.

Extracting a Hidden Message

As there is one and only image ,extraction process indicated in figure2 is much less demanding than stowing away. The stego image is obliged to spot a transporter pixel. Pixel can be checked for the content and the bits found in the message components are spared. This procedure will be proceeded until the message is totally found. In the wake of recovering the scrambled content, unscrambling will be carried out to unscramble the message.

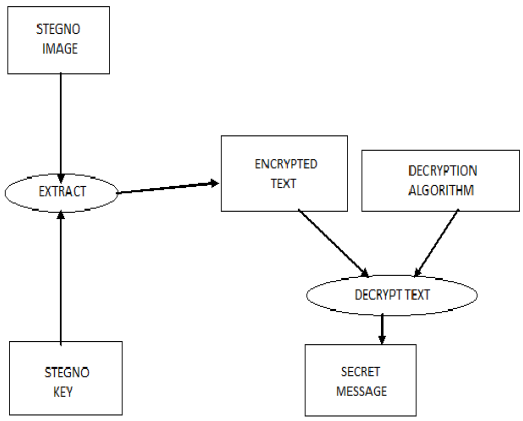

Fig 5: Extracting the Hidden message

3.3 Algorithm for Proposed Method

3.3.1 Steps to Hide the Message Using the Proposed Method:

1. Choose the proper image for the cover medium.
2. Choose the appropriate QR image (the larger segment which is having high capacity to hide the text).
3. Encrypt the required message using Quick-Response algorithm.
4. Hide the encrypted image using the COLORLSB method in the chosen cover media.
5. Send the stego image to the destination.

3.3.2 Steps to Extract the Message Using the Proposed Method:

1. De-segment the image received.
2. Select the segments in which the message is hidden.
3. De-embed the encrypted message from the QR image using the QR code.
4. After decryption, the message is available to use.

3. EXPERIMENTAL ANALYSIS

The conventional LSB strategies don't give high limit and adaptability to conceal an entire character in a solitary pixel. Generally steganography is petitioned ordinary images. By utilizing the QR Code procedure, we can give abnormal state security to the secret message against steganalysis. By utilizing figure text, this proposed technique gives better security contrasted with steganography that is generally used to conceal the ordinary content. As a whole, the investigation demonstrates that the execution of the proposed strategy is vastly improved than the current systems.

Table 1: Comparative Results

S. No.	Original Image	Regular LSB	Proposed Method
1	71.2131	71.2107	71.2133
2	91.4541	91.4515	91.454
3	116.8887	116.8766	116.8881
4	82.7183	82.7076	82.7182
5	131.8025	131.799	131.8025
6	101.9898	101.9865	101.9898
7	105.4361	105.4215	105.4353
8	91.9313	91.9226	91.9305
9	18.9911	18.9803	18.9914

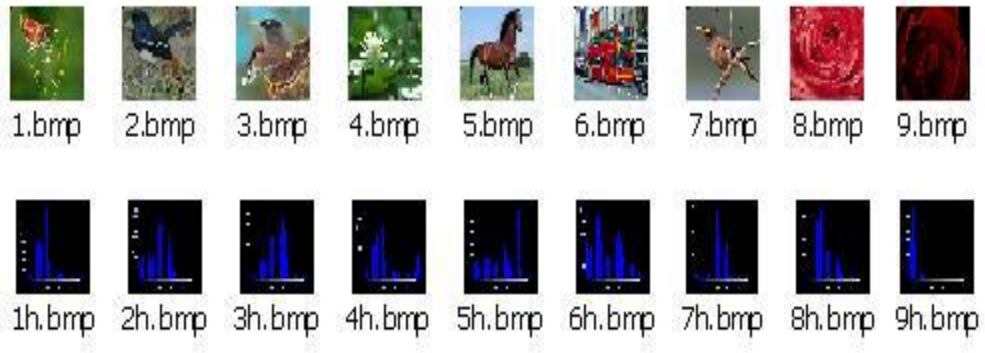

Fig 6: Original Images and its Histograms

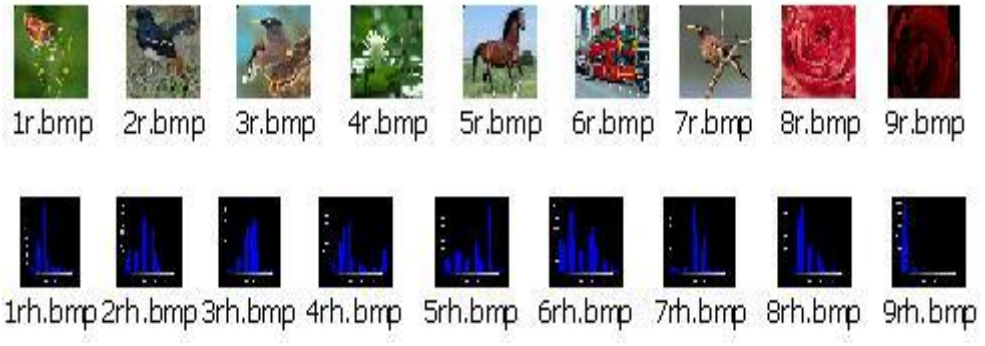

Fig 7: Regular LSB Embedded Images and its Histograms

Fig 8: Proposed COLOR LSB embedded Images and its Histograms

The above results point up that the mean of proposed technique qualities expanded than unique and customary LSB routines. At the point when a message is installed in the picture by utilizing normal LSB system, message bits are put away in pixels eight bit plane. In this way, the pixel worth does not change well. Consequently the mean estimation of image has not changed much and the quality is in respect to unique picture mean. At the point when a message is being inserted in the picture by utilizing proposed COLOR LSB and QR-code technique, message bits of single character are put away in a solitary RGB pixel. In this way, pixel quality changes a little than other implanting techniques. Notwithstanding mean estimation of proposed strategy builds respectability of message and upgrades strength of treat security. In total, the investigation demonstrates that the execution of the proposed technique is vastly improved than the current philosophies.

V. CONCLUSION

In this paper we have introduced another usual methodology of versatile steganography with higher installing limit utilizing QR Code and new LSB method. The inserting limit of the methodology is given through the substantial section size and COLOR LSB. Additionally is, this system is to an extensive degree strong with the utilization of two level securities, Steganography at the first level and Cryptography at the second level. By utilizing this novel secured component for steganography, we can give security to cloud applications like secured information transmission, session administration and so forth.

REFERENCES

[1] A Discussion of Covert Channels and Steganography by Mark Owens, March 19, 2002.

[2] Review on current steganography innovations by S. G. K. D. N. Samaratunge, seventh International Information Technology Conference, 2005, Sri Lanka.

[3] An effective shading re-indexing plan for palette based pressure by Wenjun Zeng, Jin Li and Shawmin Lei, Sharp Laboratories of America.

[4] A Review of Data Hiding in Digital Images by Eugene T. Lin and Edward J. Delp, Video and Image Processing Laboratory (VIPER), School of Electrical and Computer Engineering, Purdue University, Indiana.

[5] On the breaking points of Steganography by Ross J. Anderson, Fabien A. P. Petitcolas, IEEE Journal of chose ranges in Communications, 16(4):474-481, May 1998. Extraordinary issue on Copyright & Privacy insurance. ISSN 0733-8716).

[6] Exploring Steganography: Seeing the Unseen by Neil F. Johnson, Sushil Jajodia, George Mason University.

[7] Steganography and the Art of concealing data by Vish Krishnan, Overland Park, K.S.

[8] Information concealing – an overview by Fabien A. P. Petitcolas, Ross J. Anderson & Markus G. Kuhn (Proceedings of the IEEE – uncommon issue on insurance of media substance, 87(7):1062-1078, July 1999).

[9] An assessment of Image Based Steganography Methods by Kevin Curran, Internet Technologies Research Group, University of Ulster Karen Bailey, Institute of Technology, Letterkenny, Ireland (International Journal of Digital Evidence).

[10] Secure Error-Free Steganography for JPEG Images by Yeuan- Kuen Lee, Ling-Hwei Chen, Department of Computer and Information Science, National Chiao Tung University, 1001 Taiwan, R.O.C. Second nternational Conference on Industrial and Information Systems, ICIIS 2007, 8 – 11 August 2007, Sri Lanka 339

[11] New Steganography Technique for Palette Based Images by S.G.K.D.N. Samaratunge, University of Colombo School of Computing (UCSC), University of Colombo, Second International Conference on Industrial and Information Systems, ICIIS 2007, 8 – 11 August 2007.