An Efficient Technique for Data Hiding with use of QR Codes-Overcoming the Pros and Cons of Cryptography and Steganography to Keep the Hidden Data Secretive

Muthaiah.RM & Krishnamoorthy.N
UG Student, Dept. of CSE,
Veltech Hightech Engg College

ABSTRACT
A highly efficient technique for hiding data behind images or any other digital media and to make them more secure from the intruders is proposed. There are concepts like digital watermarking, image steganography [3], fingerprinting that are intended for the same purpose but with slight variations. In this context, cryptography can also be used to ensure security of data but the difference between the former ones and the latter, to be told in a nut shell, is the concept of steganography [9] keenly focuses on keeping the existence of a message secret whereas the cryptographic techniques revolves around keeping the contents of the message secret and safe from the intruder. There are security threats when the above said techniques are used individually to protect and keep information secret. Hence we propose a technique where we hide the data behind any digital media, here behind an image and to have its existence secretive, we put the image with hidden data into a QR code and use a powerful encryption algorithm.

General Terms
Cryptography, data hiding, steganography, water marking, QR codes.

1. INTRODUCTION
Our research paper revolves around the concept of data security. In recent times, post the rise of the internet, one of most important factors of information technology and communication has inevitably been the security of information. Today, after the fast development of multimedia technologies, the data transmission and transformation of data is more with digital media rather than analogue communication. Hence there is certainly an urge to limit the illegal accessibility of private information. In that view there are many concepts like digital image watermarking [8] ,steganography, cryptography, ciphering technique and other simple encryption and decryption techniques that vary according to the purpose and efficiency required. All the above said techniques have their own pros and cons and this paper takes up the classic and traditional method where we combine together a few techniques so as to achieve more efficiency and to have minimal shortcomings. Data Hiding is a technique used for secure communication which involves information being embedded into another object which we call as the cover object. The cover object may be an image, a video, or even a text in some cases. Fundamentally, this technique of data hiding involves the design of the embedding and the detection functions. This data hiding is analogous with the intention of the cryptographic techniques where we secure the concealment of communication and various methods have been created to encrypt and decrypt data in order to keep them secret. But since the information technology has over grown in means of the communication and its standards, it would not be enough if we keep the stuffed contents of the message secret but we also need to work on the inevitability that its existence should also be kept secret. Hence the computer techies use the concept of the steganography. The steganography [3] revolves around the art and science of invisible communications. Here we hide information into other information thus making the existence of the target data invisible. Since there are a few identified and experienced disadvantages of steganography, its success is more and more amplified when it is combined with the state of the art cryptography. In recent times, after the quick development in the technologies pertaining to the multimedia, people are concerned with the data transmission and the transformation in the digital medium when compared to the analog medium which is the obvious reason to go for the techniques to limit the illegal accessibility of the information. For this purpose we go for the techniques like digital water marking, etc., This technique of digital watermarking ,like steganography[3][5] is very strongly connected with the cryptography, all aimed at curbing the illegal accessibility of the private information from the intruders or the unauthorized users. All the above described techniques resemble each other greatly but to be noted, they also vary significantly.

The key idea of this paper is to hide data with image as the cover object. This is the typical data hiding approach through the concept of the image steganography [3]. To keep the existence of this data secret, there should be an encryption or ciphering technique that must be preferred. In this view, we use a new approach where we put this image with the hidden data into a QR code, expanded as the Quick Response code, which act as a data container. After this, we encrypt the QRC using a suitable encryption technique of our choice to keep the information secure and safe in the view of transmitting them over a communication channel or medium. The rest of the paper is organized as follows.al.

1.1 Paper organization
The section 2 brings to light the key necessity of the digital medium to be used as cover to hide the data. The section 3 gives a basic outline of the data hiding approach and its inevitability to impart safe and secure communication of the information over a medium or a channel. The section 4 compares and contrasts the concepts of the image steganography and the plain digital water marking and also delivers the author's view in a simple manner. The section 5 depicts all the technologies that are closely related with the steganography and the section 6 describes the use of the

cryptography to tauten the safekeeping of the private information. The section 7 clearly aims at the intensions of an intruder or an attacker so as to describe the thought that the intruder does not only tries to illegally retrieve the private information but sometimes to destroy the private information to blast the communication at the targeted location. The section 8 deeply examines the security threats. The section 9 characterizes the need to keep the existence of the information secret i.e. to conceal QR codes for security applications. The section 10 briefly describes the author's proposal and the section 11 discusses about the complexity in the reclamation of the data from the QRC and the section 12 tells about the practical applicability of the technique proposed and the next section describes the intrinsic worth and pro-eminence of the technique in a nut shell and the section 14 speaks about the enhancement and sturdiness of security in using our proposed technique and the section 15 concludes the paper and finally the section 16 gives the list of the references that has been used and acknowledged..

2. WHY DIGITAL MEDIUM AS A MEANS TO HIDE DATA?

It is essential that in order to hide the information, we need a data container or a cover object that may be used suitably according to the purpose. In recent times, we are using only the digital medium as the entire computer science and the communication revolves with digits rather than the analogue medium. The classic intention of all the data hiding approaches is to hide the data behind a cover object and to put them invisible. This intention was quite necessary in the ancient and early times and if found most application in the analogue form. But now, over the growth of the internet and the computer power and also the development of the digital signal processing in the area of information transmission and the communication, all the above said techniques have gone purely digital. Things have gone digital and it is most important and mandate that the techniques or the concepts used greatly satisfy the following characteristics that cannot be neglected.

1. Heftiness: It characterizes the facility to extract the embedded information from a maliciously modified cover object here an image. This shall also be called as robustness.

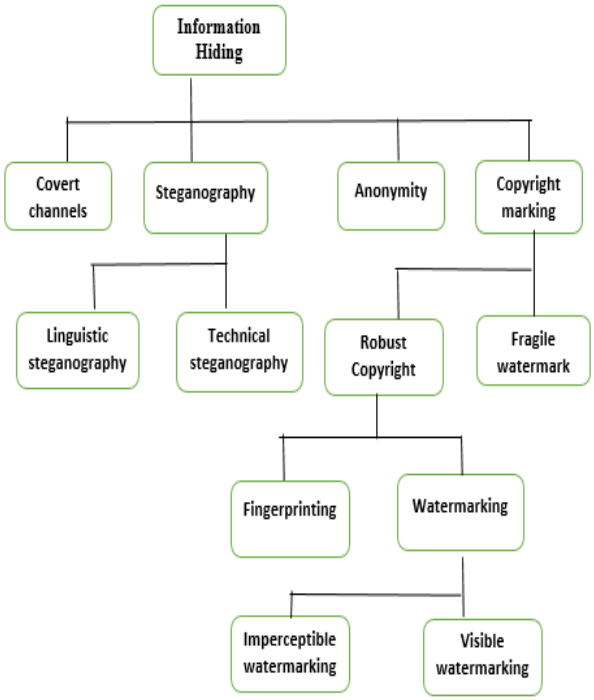
2. Imperceptibility: This corresponds to maintain the salient properties and functionalities of the cover object which here again is an image.

3. Capacity: The capacity speaks about the amount of the information that can be embedded and extracted from the cover.

All the above goals can be achieved in a digital medium but not completely. A proper trade-off shall be maintained to achieve the maximum possible efficiency.

3. OUTLINE OF DATA HIDING AND ITS IMPORTANCE

The data hiding is a form of communication in which the data to be secured is embedded into a cover object. The cover object may be an image or a video or even text at times. This technique finds use in many multimedia applications. In recent days, they are used for the ownership and the copyright protections, authentication of the ownerships, finger printing and many steganography [12] applications. The intruders are more intelligent that the technique we use must cope with them. So, we combine one technique with another so as to maximize the efficiency and to improve the performance. In this context, the digital data hiding refers to all the digital watermarking [7], image hidings and the steganographic techniques [2] as well. When using the concept of the data hiding, there should be more of integrity and the originality should be preserved so that the owner of the hidden data is sure that the data is not tampered with except a considerable amount of noise.



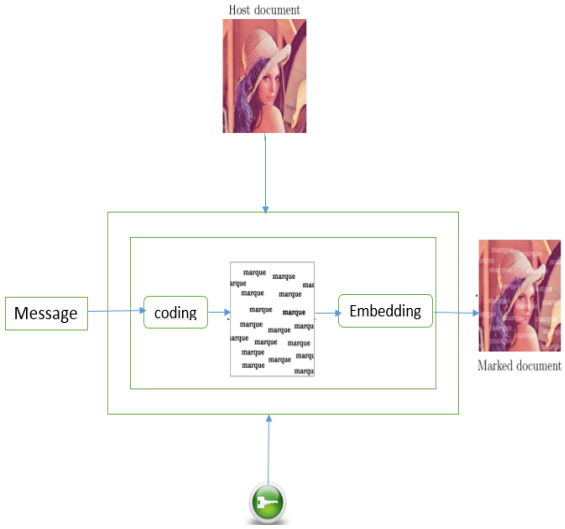
It is very evident that security is more important in the digital data hiding applications but we must be keen and cautious about the robustness and the other qualities of the data hiding technique. However, the data or information hiding revolves around three different techniques i.e., cryptography, steganography and watermarking [9] [11] [12]. Our basic idea is to combine the techniques above in order to amplify their efficiency and keep the data safe from the intruder or the attacker. The key idea is that the cover image and the stegoimage or the image with the hidden data should have a similar look.

a) Original image

b) Image with hidden data*

4. WHAT IS DIGITAL IMAGE WATER MARKING?

The digital watermarking [7] [8] strategies that hide the data in a digital media such as image, video or even the audio. The embedding of the data takes place by manipulating the various contents of the data. By this, we mean that the information is not embedded in the frame around the data. The soul concept and the success of the watermarking [5] lies in the fact that the modifications of the embedded data are imperceptible. In digital image water marking [6], we modify the pixel values of the images which should be invisible. We have also got a concept called as the digital video watermarking where we apply still image technology to each frame or we can also use methods to exploit the inherent features of the video sequence itself.



A model depicting watermarking process

4.1 Security threats in watermarking

The nature of the multimedia objects are fragile and flexible [6] that had actually led to the development of the technologies to this wider. There are a few important properties that are to be considered. The first and foremost is the image fidelity. There should be no obvious difference in the image fidelity because if a slight difference is noted, it will be easy for an attacker to extract the information in it or to destroy the information contained in it.

The next issue is the transparency. Here, we need to ensure that the embedded data is not perceptually degrading the underlying content. We must also consider and be cautious on the note that the data that is embedded has not been tampered with or forged or even removed at the worst case. This is actually the area of the research where it has evolved to a greater extent but a few more significant problems are to be solved. To put in a nut shell, in digital watermarking[4][5], the watermark is hidden in the host data such that it should be inseparable from the data so that it can be defiant to many operations but do not degrade the host medium of the data. Thus in some way, this techniques derives from steganography which means covered writing.

5. IMAGE STEGANOGRAPHY AND DIGITAL WATERMARKING

It is said that the steganographic [11][1] techniques are not as robust as digital water marking since the data embedded cannot be completely protected against the technical modifications whereas with the digital watermarking techniques[8], it is possible to have more resilience. Even though the existence of the information is known, it is eventually hard for an attacker to destroy the data that is embedded in the cover object without complete knowledge of the key. We should also make note of the implication that the watermarking [5] strategy can embed typically much less information into the cover data than the steganographic methods.

6. TECHNOLOGIES CLOSELY ASSOCIATED TO STEGANOGRAPHY

The steganography [9][11] and its closely related are the encryption technique. Both these techniques are actually used to ensure the confidentiality of the data. However, the significant difference between those two is that with encryption of the data anybody can notice that both the parties are communicating secretly. This is the primary reason where steganography has an edge over the encryption technique and hence it finds application in the copyright marking. When using the steganography as a means to hide to data into a cover object, the integrity of the hidden information after it has been embedded into the stego object must be correct. The hidden information should not be changed in whatever means such as the additional information being added or the loss of the information or even a change or modification to the actual hidden information.

The steganography can be divided into two. One is the fragile steganography. In this type of the steganography, we embed the information into a cover object which gets destroyed if the cover is modified. This method cannot be used for many applications since it can be easily removed. The other is the robust steganography in which the data is embedded into a file that cannot be easily destroyed. By this we do not mean that it is indestructible but the amount of work that has to be done to extract the exact information will render the file completely

useless. Hence the mark shall be hidden in a part of the file such that its removal could be easily perceived.

7. CRYPTOGRAPHY TO TAUTEN SAFEKEEPING

In order to ensure the safekeeping of the information, it is preferred to use the cryptographic techniques [17]. At this point, we must know the various attacks that the data embedded will face. The first and foremost shall be the active attacks where the intruder tries to remove the data or make it undetectable. The next shall be the passive attacks where the intruder's intention is to detect the presence of embedded data but not to extract it. The next shall be the collision attack where the hacker intends to remove the watermark by targeting the cover object with many other watermarks. The final one shall be the forgery attack which occur in the worst case. In order to avoid all these attacks, it is inevitable to use the cryptographic techniques. The cryptography that amplifies and brings about sound data hiding finds application in content identification and management, forensics and piracy deterrence and content filtering. The cryptography shall be combined with the image steganography [9] [10] for document and image security and improved auditing.

8. INTENSION OF AN INTRUDER OR ATTACKER

The intension of an intelligent intruder need not only be extracting the embedded data but also to detect its presence and also to destroy the purpose. For example, if we are intending to transmit the data over a communication channel and the data that we need to transmit is very confidential and sensitive, we go for techniques like steganography or any other classic data hiding method together with the cryptography or the other encryption technique. In such instances, the intruder could do nothing from the information but could destroy the entire communication detecting the presence of the information. Hence, we need to maintain the secrecy of the existence also. Thus, the technique that we use to safe keep the data must be robust and fight against all the cryptanalytic attacks destroying all the intentions of the attacker what so ever it be.

9. NEED TO CONCEAL QR CODES FOR SECURITY APPLICATIONS

9.1 Quick Response Codes

Since last few years, two-dimensional (2D) codes have gained the attention of the people from the industrial backgrounds and gradually replaced one-dimensional bar codes in many applications due to their higher information storage capacity. QR code is hence as an information container which can be captured and decoded by smart phones directly.

Quick response (QR) codes, defined by the ISO/IEC18004 standard, are one of the most popular types of 2D codes. Thus, Quick response codes (QR Codes) are two-dimensional barcodes designed to share encoded information in a variety of formats. QR code is just a matrix bar code containing much more amount of information than its 1D counterpart a typical QR code is a square black and white pixelated box. Encoded information may contain simple text, graphics, or direct users to a website or landing page for additional information. Furthermore Barcode technology is superior in speed, steadfastness, information capacity, universality, and cost. The two dimensional code can encode in 2-D directions, represent thousands of characters, and bear a certain automatic error correction capability. The information in the code can be encrypted, which needs special software to decipher and decode, which ensure better security. Quick Response codes, QR code for short, is a two-dimensional barcode with high information density, error correction ability and convenient encryption mechanism.

9.2 Transformation in QR's applications

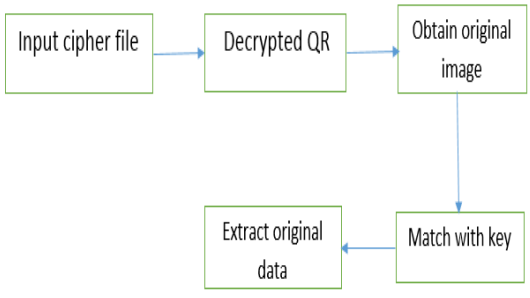
The QR code shall easily be seen in web pages or on posters nowadays. It is a two-dimensional code in square shape, mostly represented by binary form (black and white pixels). It is easily recognizable because it looks like a random pattern. Colorized QR codes too are in existence. The beautifications of QR codes have also been proposed recently. During the origination of the QR codes[16], the purpose was to utilize the quick connection to the specific web page with the URL information converted to the QR code[13][15] pattern. But these days they stand as data containers that provide more security when encrypted since from the viewpoint of data hiding researches, QR code shall then be regarded as the visible watermarks. The above is the reason why we use QR code as a data container and encrypt it in our proposed application.

10. PROPOSED TECHNIQUE

Considering all the above said pros and cons of all the techniques like data hiding, image steganography[1], cryptography and various other encryption techniques like the Triple-DES and Blowfish etc., we propose a technique that has greater practical applicability and pro-eminence. In our proposed technique, we first watermark and embed the data onto the image which we use as the digital cover object. That is we hide the data to be secured into an image which is called as the image hiding or some means of the steganography [10]. Now, after this step, we put this image in the Quick Response code which act as a data container and hold the image with the embedded data. We now use an encryption technique to cipher the QR code [13][15] to protect it from the cryptanalytic attacks from the intruders. Now, this can be transmitted over the transmitting medium or the communication channel. In the receiving end the receiver should know the key with which the image is watermarked but before that he should be aware of the cipher with which the QR code[13][14] was encrypted. By using the proposed technique, we nullify the chance of passive and the active attacks discussed above.

11. RECLAMATION OF DATA FROM DIGITAL MEDIUM

In order to reclaim the data that has been stored in the image, the reverse process has to be done as with all the other traditional techniques. This is depicted as follows.



12. PRACTICAL APPLICABILITY AND PRE-EMINENCE OF THE PROPOSAL

The technique that we have proposed has got an immense applicability practically and hence this technique shall be used widely. We enlighten this because we use a very strong technique that stands against loss of information with an intention to disallow the cryptanalytic attacks any further. Another exclusive benefit of our proposed technique is that the transmission cost is comparatively less since we transfer a large amount of data into a single QR container and then apply the encryption algorithm rather than apply the encryption algorithm to the data itself. Hence the technique shall be of greater use in the nearest future.

13. CONCLUSION

In this paper, all the pros and cons of the techniques like the image steganography[9], data and image hidings, cryptography, finger printing and other encryption techniques were brought to light and a technique where concealment of the data into the QR code[13][14][15] so as to provide more security to the embedded data is proposed. The technique's scope and the practical applicability was also discussed and a comparative study was made between all the said techniques. Furthermore, this method could be used in the transmission of the big data overcoming the shortfalls of the digital media and the associated security techniques, which could be an extension of this paper, in future.

14. REFERENCES

[1] J. Fridrich, Multimedia Security Technologies for Digital Rights Management. Academic Press, 2006, ch. Steganalysis, pp.349–381.

[2] J. Fridrich, R. Du, and M. Long, "Steganalysis of LSB encoding in color images," in Proceedings of the IEEE International Conference on Multimedia and Expo. New York, USA: IEEE Computer Society Press, 2000.

[3] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique" International Journal of Computer Applications ISSN 0975 – 8887, Volume 9– No.7, November 2010

[4] Q. Li and E. Chang. On the possibility of non-invertible watermark schemes. In Proc. of IHW'04, Lecture Notes in Computer Science, volume 3200, Springer-Verlag, 2004.

[5] Cox I. J., Miller M. L. et al., Digital watermarking and steganography, Morgan Kaufmann Publishers (2008).

[6] ZuneraJalil, M. ArfanJaffar, and Anwar M. Mirza, "A Novel Text Watermarking Algorithm Using Image Watermark", International Journal of Innovative Computing, Information and Control (IJICIC) (indexed by ISI with Impact Factor 2.93) (Scheduled to be published in February, 2011)

[7] Dr. Martin Kutter and Dr. Frederic Jordan, "Digital Watermarking Technology", in AlpVision, Switzerland, pp 1 – 4.

[8] Harpuneet Kaur, R. S. Salaria, "Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data", The IASTED International Conference on Communication, Network, and Information Security (CNIS–2006), MIT, Cambridge, Massachusetts, USA, Oct 9–11, 2006. (Communicated)

[9] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science.

[10] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[11] Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003

[12] Venkatraman, S., Abraham, A. & Paprzycki, M., "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004

[13] QR Code, Available at: www.qrcode.com

[14] QR-Code Generator, http://qrcode.kaywa.com/, 2010.

[15] International Standard. ISO/IEC 18004. Information technology --Automatic identification and data capture techniques -- QR Code 2005 bar code symbology specification. Second Edition. 2006-09-01.

[16] GB/T 18284-2000 "Quick Response Code",Beijing, National Standards Press, 2000

[17] W. Stallings., "Cryptography and Network Security: Principles and Practice," Prentice-Hall, New Jersey, 1999.