

Enhanced QR Code Covert Communication with Dual Security & Robust Detection

Tarun Kumar Bhandari¹, Luv Sharma², Khushal Chandra Agrawal³

¹ M.Tech Electronics And Communication, S.S College of Engineering, Udaipur

² Assistant Professor Department of Electronics and Communication, S.S College of Engineering, Udaipur,

³ Assistant manager (E&I), Udaipur Cement Works Ltd, Dabok, Udaipur

Abstract: Covert communication is the backbone of intelligence fraternity with the rapid advancement in technology, newer & innovative methods of covert communication are required QR code is a rapidly emerging technique for communication of small data such as web links, address, location, any short text or small Images / Logos. QR Code also provide the advantages of being electronically readable specially through mobile phone camera and mobile phone has become an indispensable part of modern life, a covert communication system based on QR Code is highly anticipated. The author has proposed a highly secure QR Code communication system with dual security employing mixed key Cryptography & attack resistant watermarking techniques. Also the author proposes to test the system with various types of image attack & their results on recovered QR Codes & their readability on mobile devices.

Keywords: Enhanced QR Code, Covert Communication, Cryptography, Watermarking, Robust Detection.

I. INTRODUCTION

In computer security, a secret channel is a type of attack that creates the ability to move information objects between processes that are not allowed to communicate by the computer security policy. The term, created in 1973 by Lampson, was defined as "absolutely non-transferable channels, such as the impact of the service program on system load", to distinguish it from legitimate channels subject to access controls by COMPUSEC. The secret channel is called hidden from access control mechanisms for secure operating systems because it does not use legitimate computer data transfer mechanisms (usually read and write) and therefore cannot be detected or controlled by the security mechanisms that form the basis of secure operating systems. It is very difficult to install secret channels in real systems, often detected by monitoring system performance. In addition, they suffer from low signal-to-noise rates and low data rates (typically, at a few bits per second). They can also be manually removed with a high degree of assurance from secure systems through well-established secret channel analysis strategies.

II. OBJECTIVES OF STUDY

- [1.] Design and development of an efficient mobile device information exchange system, using mobile LCD/TFT display.
- [2.] The proposed system should be able to take small information such as text weblink etc, & convert it to a pattern on device screen readable by camera of another device.
- [3.] Inc operation of emerging technology & trends such as QR code instead of bar code to exchange as normal without alerting any observer.
- [4.] Enhancing the security of messaging scheme by incorporating state of the art cryptography technologies. Sundering un authorized reception highly without having pre-shared cryptographic key.
- [5.] Improving the efficiency of the system by embedding the secure graphical code in a cover image using linear bit replacement steganography.
- [6.] The proposed system should be immune to various types of image attacks such as cropping, compression, tompement, enhancement etc.
- [7.] The proposed system can be optionally aimed of reduction of time & space complexity of existing approach.

III. EXISTING TECHNIQUES

In this article, Key Lock is integrated into the differential shift by multiplying the orthogonal frequency division so that the data flow can be edited into two-dimensional bar codes. It has been shown that the QPSK-OFDM modification camera has serious disadvantages in reducing LCD movements as the phase of each component is constantly changing. On the other hand, the addition of off-DM differential phase modulation to the data stream modification in the adjacent phase variations (DPSK-OFDM) rapidly reduces the mobility effect due to the gradual change from one element to another, contributing to the deviation. happens. From the ideal phase of the received signal. [1]

Bad PDF files have become a popular threat in recent years. PDF documents are a very effective attack vector for cybercriminals. Despite the efforts of software vendors like Adobe, PDF programs often suffer from zero-day attacks. In

this work, we introduced a new approach based on information and content-based information designed to provide the most accurate identification of harmful PDF programs. We have also shown that our methodology, with a careful selection of algorithm learning, is also capable of counteracting theft attacks. Finally, our task, clearly to counter malware attacks, clearly illustrates the need for safe learning techniques for malware detection. [2]

QR codes are the most popular bar codes that are most useful in all situations. The paper went through two different and different 2D barcode formats and found that QR codes work well. Color features are now integrated with QR codes to improve their performance. The use of colors will increase the data rate as well as the complexity of the decoding. Although bit error rates and therefore information capabilities vary as a result of the three channels, the error rates in bands are easily processed by the available debugging options for a color bar code. Decryption can be adopted effectively. Security issues are still an issue. Access to the QR code in the LAN can cause privacy issues. The solution lies in the developing part. We can go over the classic encryption techniques to solve this. Share DenisView A secure method has recently been introduced but its details are not yet known. [3]

The cloud security algorithm for cloud computing environments has to use cloud servers for time and memory constraints during server encryption and decryption. So it's best to encrypt the data stored in cloud servers such as AES, and then encrypt the secret key with a dual algorithm to share the actions. [4]

The use of QR codes in education is still in its early stages. Planning and preparing the right material to be created in the QR code is a daunting task for the teacher, especially if we don't know the QR codes. It takes a lot of teacher time to make sure that everyone in the class knows how to use it. Teachers should consider the teaching aspect of teaching in QR code design rather than techniques. The focus should be on learners rather than on technology. If not well planned, the entire lesson will fail to motivate students. [5]

This paper describes the various attacks by using the QR code. Since each technology has its benefits and limitations, QR codes are also. Because QR codes are gaining popularity, their misuse is increasing day by day. QR codes are commonly used in ads and payments. Therefore, along with this use, security issues also arise. There are different ways to address different security issues related to QR codes. Synchronous and ambiguous data markup can also be implemented using QR codes. [6]

A record number of competitors and participants were registered throughout this year's challenge. User feedback was critical during the initial stages and in identifying problems with the new recording environment. An important concern was that the training dataset was too easy or unrepresentative for the entire test groups (see Table 3). The challenge FAQ has been updated to suggest ways to increase the training package (eg using the MGH / MF database available on PhysioNet [12]), which has helped some competitors. Most of the top entries use pulse information, which results in a small advantage of up to 5% in a C model entry that uses only one ECG signal. [7]

In this chapter, we present a necessary and sufficient condition for carpet critical points to exist for a wide range of straight vector fields. The presence of a critical point allows us to develop a powerful method for detecting critical points in n dimensions. Moreover, when giving accurate accuracy values, this technique is guaranteed to use the specified accuracy, so the result can be calculated in a completely uniform manner. In the future, we would like to achieve more in the category of interpolation functions for which we have shown this result, and identify other interpolation techniques that fall into this category. We would also like to extend this work to include the critical points classification. [8]

By viewing all the above analysis, it can be said that the product is a system based on a highly efficient GUI. After finishing the project, we can make sure to overcome the current system problems. The advanced student ID card is created for the computerized QR student to increase efficiency and reduce error for humans. All records and data are stored in the Microsoft SQL Server QuickStart Studio database, from which data can be easily deleted and retrieved. Editing is also flexible because the authority just needs to provide the required information, then print an identity card with the student's photo with the real-time video stream and enter a QR code that contains detailed student information that can be scanned in one second using a smartphone. [9]

Using a QR code marketing strategy, while it is simple, will add value to the company. QR codes provide businesses with an effective way to advertise their products that cannot be copied to a printed page or billboard. QR codes can engage customers much better than traditional print ads. Based on the multimedia framework Yes. We can note that the QR code fits the application of hybrid channel technology. Marketers need to integrate better mobile devices and networks into the mobile Internet platform to provide an easy and fun experience for a smooth transition from one network to another. Furthermore, type A communication, which includes a hybrid approach with intensive interaction, can produce the best results for using a QR code for marketing purposes. Type B should only be used for informational purposes in High Involvement products, where consumers need more information to make a purchase decision. [10]

In this work, we proposed a new detector for detecting solid boxes (dust, dirt, and stains) that focuses specifically on providing low alarm rates. The proposed potential approach combines several ongoing initiatives and better conserves information in ways that utilize the initial bilateral decision. The initial SFD response map has been adapted to provide consistent reliability values by changing the SDIa method. The new collaborative engine is an effective tool for increasing durability against noise and movie noise. Further, it has a positive effect on the local completion of potential SFD boxes. Finally, we apply a set of specially tailored samples to identify areas that are likely to cause false alarms. These prevention measures are based on analysis of the local motion and image field and provide a strong cushion of SFD response maps in pathology areas (obstruction, detection, moving edge areas, etc.). A reasonable diagnosis shows that the proposed FAR detector achieves a much lower error detection rate than the modern SFD detection algorithm. [11]

IV. METHODOLOGY

System Block Diagram

(A) Transmission block

In this transmission block diagram we can see 1st used secret text message as input then QR code will be generate then encrypt this QR code then embedded this QR code in the cover image. In this block diagram we can see random seed key generation is used for generate private key and by using this private key we encrypt QR code. And we can also see we are input cover image then gray scale conversion & RGB recom position process will be done then QR is embedded with cover image.

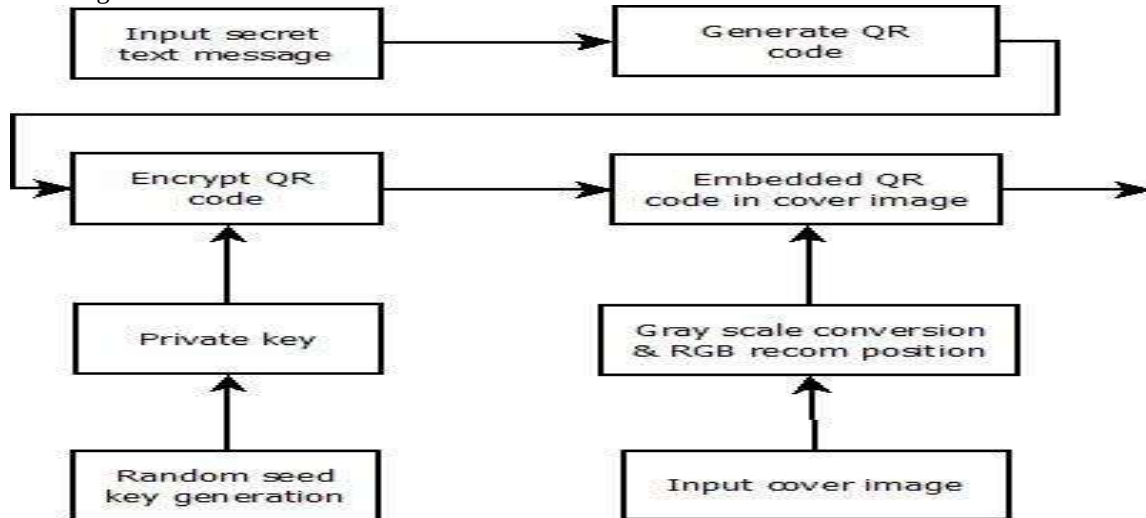


Fig: 1.1 Transmission Block diagram

(B) Attack Block Diagram

In this block diagram we can see 1st cover image with embedded data then four things do with this that is image crop attach, noise addition attach, contrast change attach, compassion attach, tomperment attach then degrade cover image after attach.

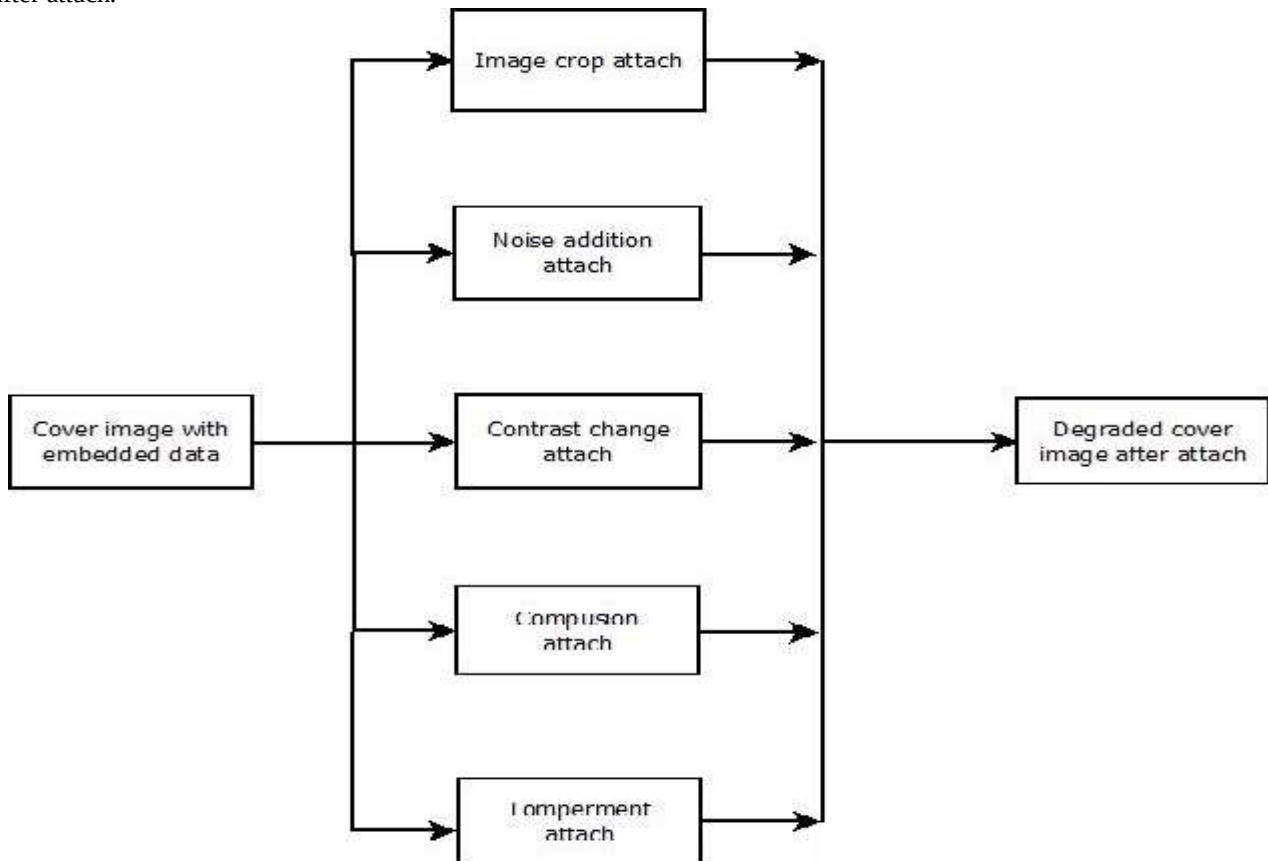


Fig: 1.2 Attack Block diagram

(C) Reception block

In this block diagram we can see 1st degraded cover image with hidden data then de-watermark embedded QR code then decrypt QR code with pre-shared private key then we have QR code which is easily read by mobile device.

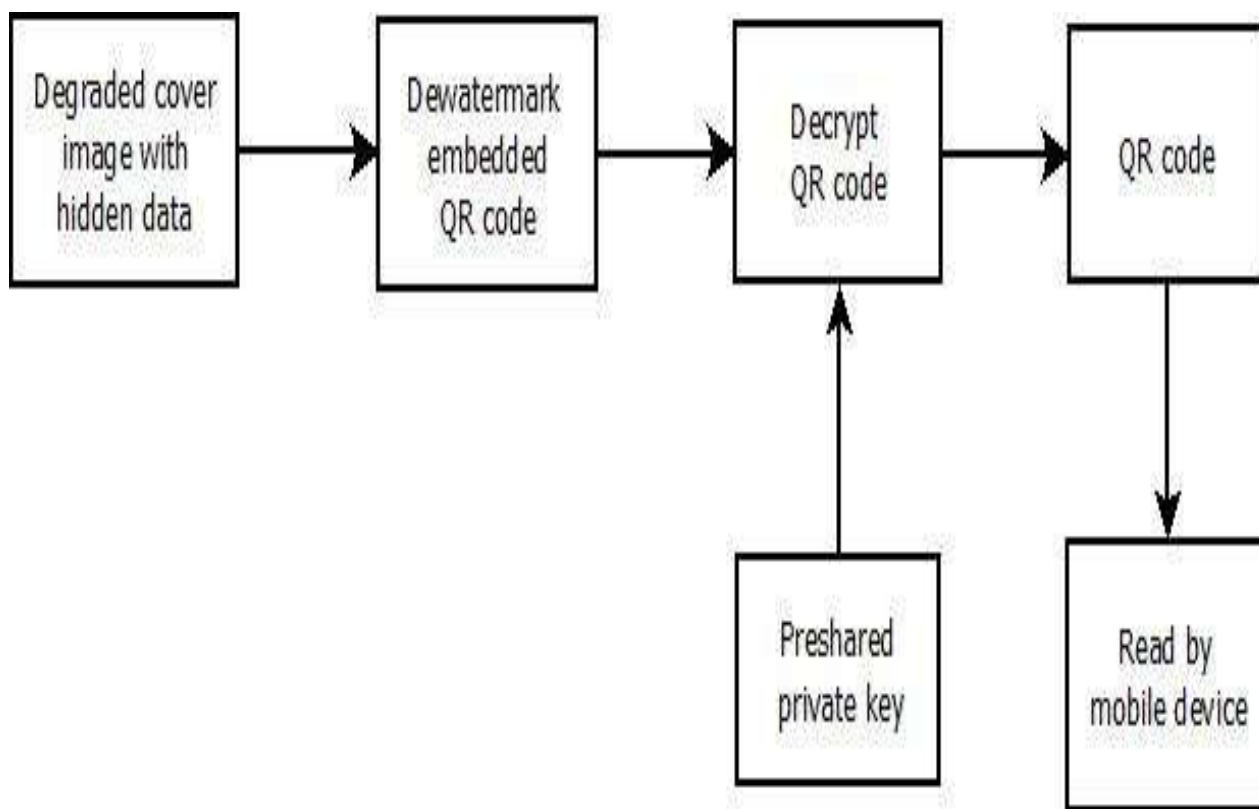


Fig: 1.3 Reception Block diagram

V. RESULTS

In this window we can see the text of secret code that is Hello how are you.

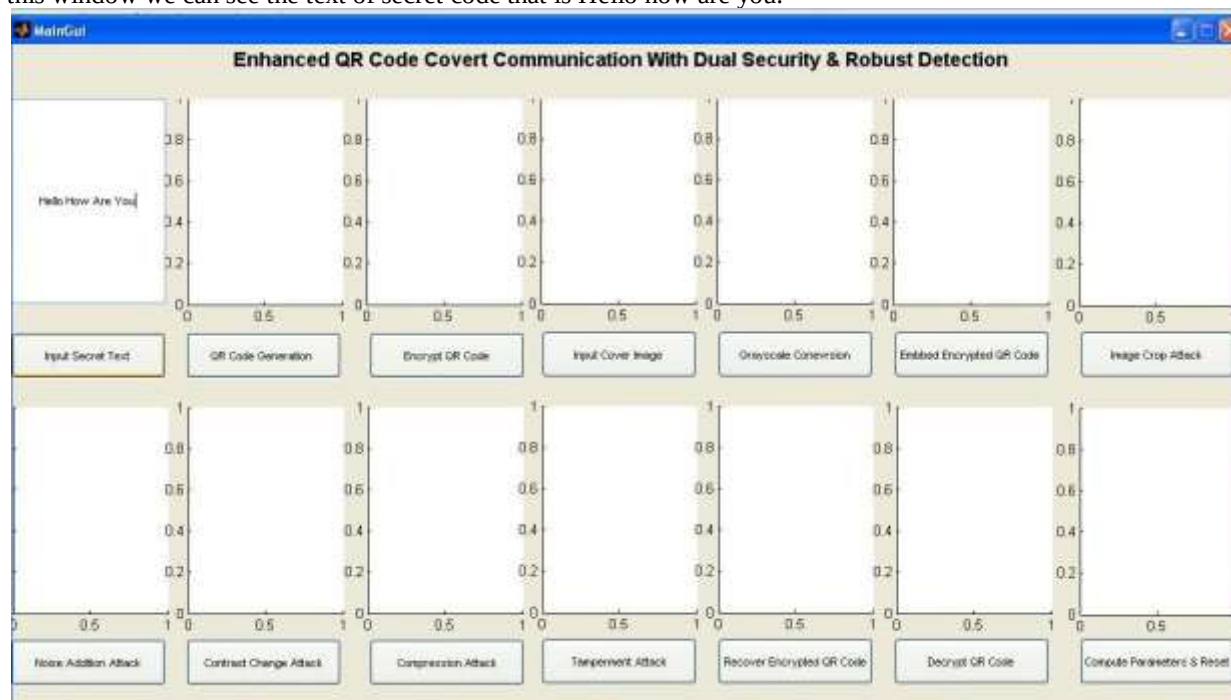


Fig 5.1 Secret Code

In this window we can see that QR code is converted into a encrypted code.

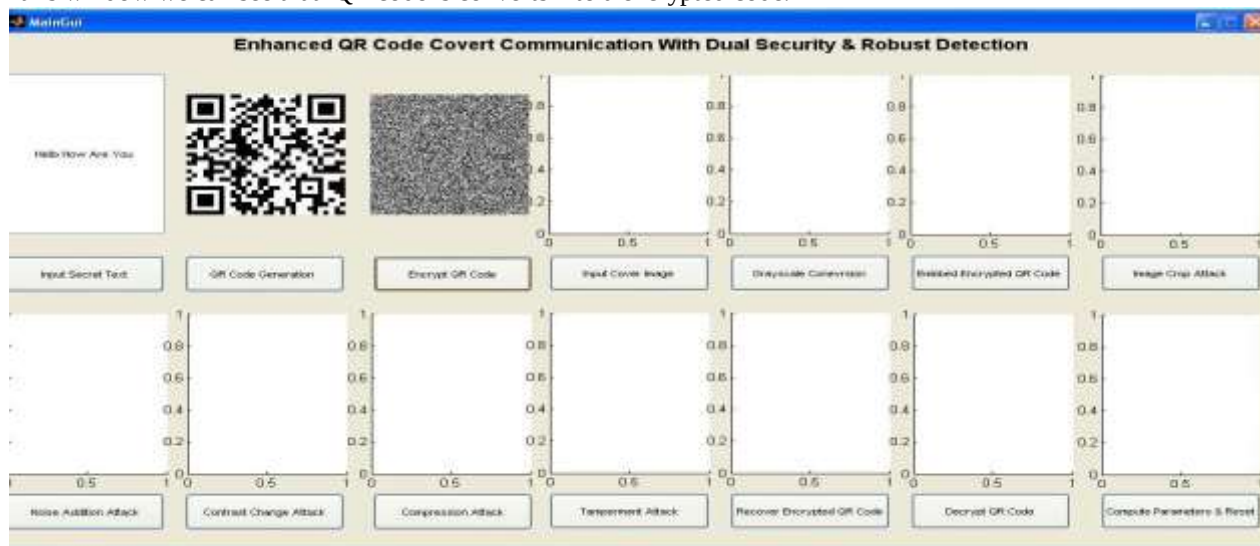


Fig 5.2 Encrypt QR Code

In this window we can see that our input image is sunset site and we can also see gray scale image of this input image.

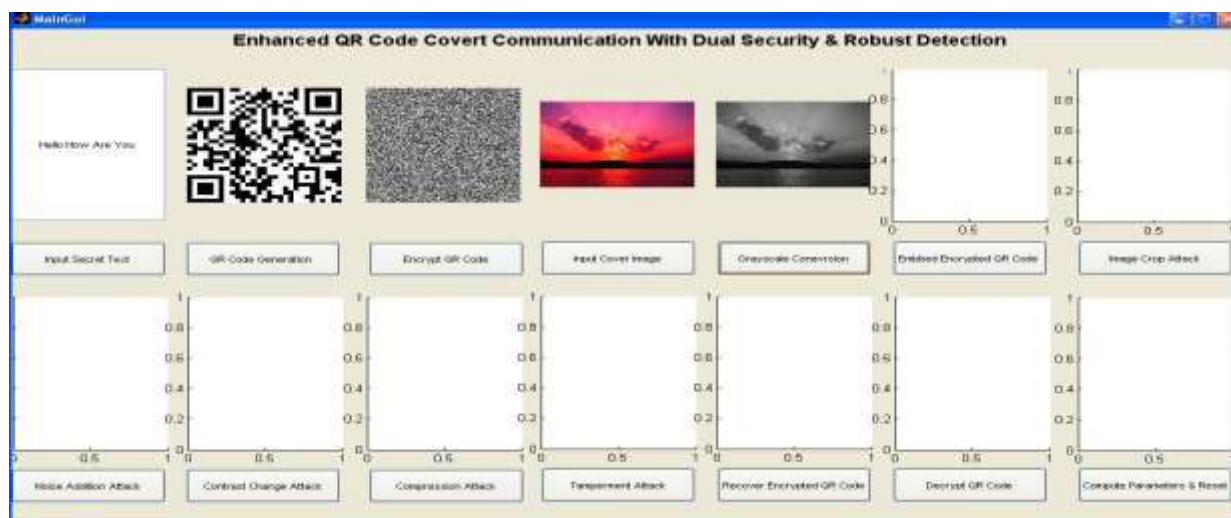


Fig.5.3 Gray Scale Image of Input Image

In this window we can see input cover image, grayscale image change and embedded encrypted QR code image.

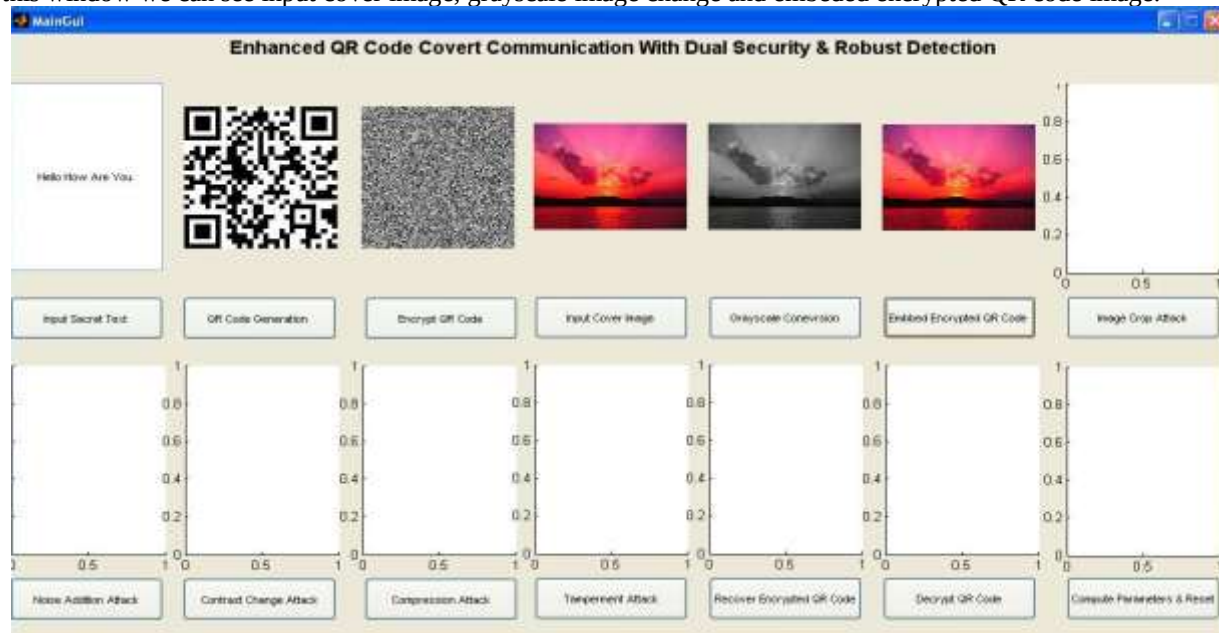


Fig.5.4 Embedded Encrypted QR Code

In this window we can see recover encrypted QR code.

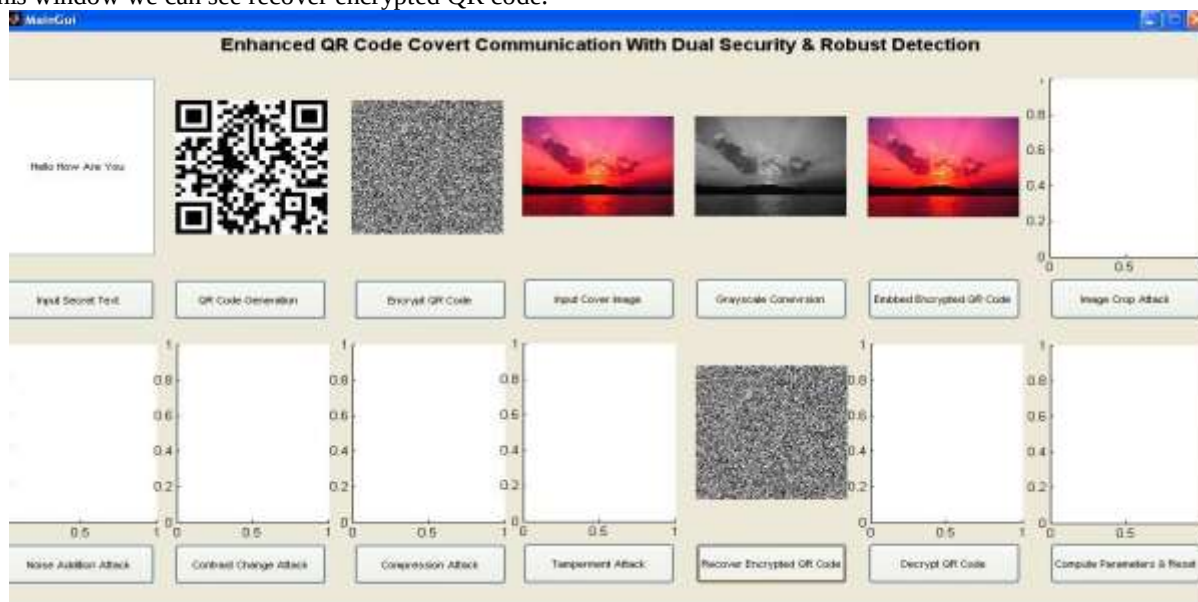


Fig.5.5 Recover Encrypted QR Code

In this window we can see original image snr, original image nse, recover image snr, recover image nse.

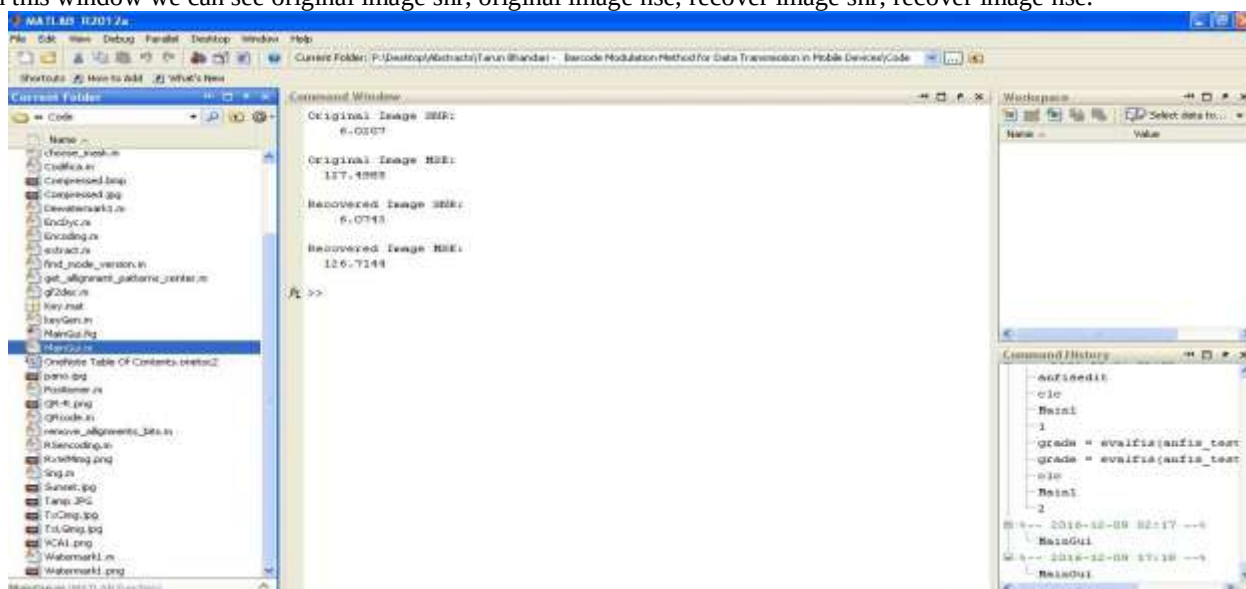


Fig.5.6 SNR and NSE

In this window we can see recover encrypted QR code and decrypt QR code.

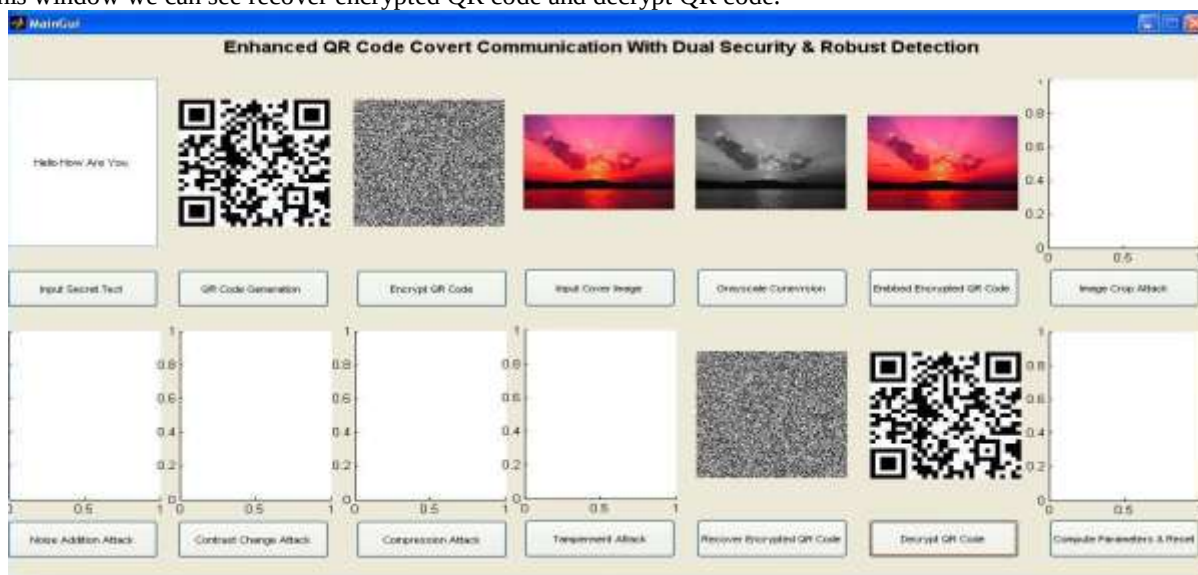


Fig 5.7 Decrypt QR Code

CONCLUSIONS

The author has proposed a unique & robust method of enhanced QR code covert communication with dual security & robust detection. As covert communication saves as lifeline for intelligence gathering commonly & counter intelligence measures are highly evolved latest & innovative techniques are required for enhancing covert communication capabilities. QR code has rapidly gained popularity for small data exchange via image scanning techniques particularly through mobile phones & thus has provided a potential medium for covert communications using QR code. Also QR code being electronically generate able & readable thus enables easy exchange of information through portable devices without generating any paper trail. The covert QR code security is stepped up by encrypting the QR code employing mixed key cryptography using a private key. The private key must be pre shared with the receiver so as to enable him to decoding QR code. The covertness of QR code is further enhanced by employing a attack resistant water marking technique to hide the QR code into a cover image. As demonstrated by the result the proposed system has been successfully implemented in MATLAB 2012. Also the proposed system has been subjected to various types of image attacks & their affect on recovered QR code MSE (Mean Square Error) & SNR (Signal to Noise Ratio) is observed. Successful recovery of QR code & its decoding & extraction of encoded information is achieved with a minimal loss of information after various types of attacks employed.

FUTURE SCOPES

The author has demonstrated a reliable secure & robust covert communication technique for mobile device information interchange. As the technology is rapidly evolving & counter intelligence techniques are advancing there is a requirement of constant evolution of covert communication techniques. One of the primarily sought improvements would be to secure the encryption using biometrics as finger print sensing is available in most of the modern mobile phones today. Another important addition could be addition of QR code itself as a cover image to hide another encrypted QR. Also the proposed technique can be improved to hide low resolution images or gifs instead of text only.

REFERENCES

- [1.] Amin Motahari, Malek Adjouadi “Barcode Modulation Method for Data Transmission in Mobile Devices” IEEE TRANSACTIONS ON MULTIMEDIA 2015.
- [2.] Davide Maiorca, Davide Ariu, Iginio Corona and Giorgio Giacinto “A Structural and Content-based Approach for a Precise and Robust Detection of Malicious ” SCITEPRESS 2015.
- [3.] Arya Chandran S “Review on Color QR Codes: Decoding Challenges and Security Issues” International Journal of Engineering Research & Technology (IJERT) 2014.
- [4.] Uma Naik, V. C. Kotak “Security Issues with Implementation of RSA and Proposed Dual Security Algorithm for Cloud Computing” IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 2014.
- [5.] Abby Ashraff Saprudin, Norlia Goolamally, Latifah Abdol Latif “EMBEDDING QR CODES IN THE TEACHING AND LEARNING PROCESS” Seminar Kebangsaan Pembelajaran Sepanjang Hayat 2014.
- [6.] Shruti Ahuja “QR Codes and Security Concerns” Shruti Ahuja / (IJCSIT) International Journal of Computer Science and Information Technologies 2014.
- [7.] George Moody, Benjamin Moody, Ikaro Silva “Robust Detection of Heart Beats in Multimodal Data: The PhysioNet/Computing in Cardiology Challenge 2014” ISSN 2014.
- [8.] Harsh Bhatia, Attila Gyulassy, Hao Wang, Peer-Timo Bremer, and Valerio Pascucci “Robust Detection of Singularities in Vector Fields” Springer International Publishing 2014.
- [9.] Md. Sanaul Haque, Richard Dybowski “Advanced QR Code Based Identity Card: A New Era for Generating Student ID Card in Developing Countries” IEEE 2014.
- [10.] Teuta Cata, Payal S. Patel and Toru Sakaguchi “QR Code: A New Opportunity for Effective Mobile Marketing” IBIMA Publishing 2013.
- [11.] Stefanie Wechtitsch, Hannes Fassold, Peter Schallauer “Robust Detection of Single-frame Defects in Archived Film” IAPR 2012.