**. Literature Survey**

**Image Embedding in QR Code:**

The QR (Quick Response) code is a two-dimensional barcode developed by the Japanese company Denso-Wave in 1994, and was approved as an ISO International Standard and Chinese National Standard in 2000. The QR code has been widely used due to its good features such as large data capacity, high speed scan, and small printout size. Increase in number of smart phones is the reason behind popularity of QR code. Smart phones are capable of decoding and accessing on line resources as well as it has high storage capacity and high speed of decoding. QR codes are used in a various applications, such as accessing websites, initiate phone calls, reproduce videos or open text documents and data storing purposes. An important problem of QR codes is its noisy looks. To improve the appearance of QR code and to reduce noisy black and white random texture has generated great interest for algorithms capable of embedding QR codes into images without losing decoding robustness. There have been many efforts to improve the appearance of such embeddings. The main challenge of any embedding method is the embedded result should be decodable by standard applications. The embedding introduces changes in the luminance of the code, distorting the binarization thresholds and thus increasing the probability of detection error. The second challenge is the problem of using the entire area of the code in which the image or logo is to be embedded. This cannot be done by simply replacing information modules with the desired image. A good embedding method should decrease the number of corrupted modules and uses the utmost area. The proposed method is based on the selection of a set of pixels using genetic algorithm. The concentration of pixels and its corresponding luminance are optimized to minimize a visual distortion. Distortion metric is subject to a constraint in the probability of error.

QR code consists of black and white square blocks called as modules of a QR code. Each module is assigned a single bit value. Information is encoded into the QR modules. A dark module is binary one and a light module is binary zero. A codeword contains 8 bits of information. There are 40 versions of QR code. A QR code with version V have (17 + 4V) × (17 + 4V) number of modules. Therefore version 1 has 21 × 21 modules whereas version 40 corresponds to 177 × 177 modules. Fig. 1 shows the structure of a QR code. Finder pattern contains three identical square shape located at the three corners of QR code. Finder pattern is the most important pattern which enables the detection of QR code. Alignment patterns are also essential to locate, rotate and aligning the QR code. Finder pattern, timing pattern and alignment pattern are collectively known as function pattern region of QR code. Alignment patterns are observed with version number 2 and onwards however version number 1 does not have any alignment pattern. Encoding region within the green color consists of data and error correction code words. Data code words are of two types i.e. information code words which stores the actual information and the second is padding code words. Encoding region stores the data, parity modules and decoding information in the form of a code words. A codeword consist of a block of 8 modules. Quite Zone is the guard region of QR code. QR code utilizes RS (Reed Solomon) codes for error correction. A QR code contains multiple RS codes where one RS code is sufficient to store the message. The remaining RS codes are usually used to store non meaningful messages [2]. There are 4 types of error correction level i.e. L, M, Q and H which can recover 7%, 15%, 25% and 30% of errors in the code words respectively.

There have been a lot of efforts to improve the appearance of QR code. The base strategy of such work is to find the best group of QR modules to substitute by the image or logo in the QR code. The method presented in [3] proposed that, there are three areas to replace the QR module by the image or logo. These areas include data codewords, padding codewords and the error correcting codewords. Depending on the error correction level of QR code, pad characters have been changed. The size of the embedding image in the QR code is identified and then the image is implanted in the identified region of QR code. The size of the image which is to be embedded is increased and tested the readability of QR embedding to find largest size of which the image could be embedded except the finder pattern of QR code. Author concludes that if the numbers of characters in the QR code is decreased then the larger image can be embedded. The second approach [12] of embedding is based on the modification of the pixel’s luminance. The luminance of central pixels is modified since this is the area usually sampled by the decoder. This approach uses the entire area of the code for embedding except the finder and alignment pattern. The approach in [10] performs the blending which combines the color image C and the QR code Q based on the luminance of color image and the binary value of QR code. The blending of C and Q to produce an output B is accomplished by replacing pixels of Q with those of C. Author assumes that pixels of Q are normalized so that white pixels have a luminance of 1, and black pixels have a luminance of 0. This algorithm ensures that the blended output image preserves the bright part of color image when the pixel value of the QR code equals to 1, and dark part of the color image when pixel value is 0. Cox proposed a complicated algorithm [19] to embed a binary image into a QR code during the data encoding stage of generating the code. He carefully investigated the internal structure of QR code and the logic behind data encoding, and designed an algorithm to encode image content as redundant numeric strings appended to the original data. However this technique works only for URL type data string and the quality of embedded image is limited by the length of encoded URL.

**Robust Message Hiding for QR Code:**

Response Code (QR code) is widely used in daily life in recent years because it has high capacity encoding of data, damage resistance, fast decoding and other good characteristics. vSince it is popular, people can use it to transmit secret information without inspection. The development of steganography in QR code lead to many problems arising. How to keep the original content of QR code and embed secret information into it are the two main challenges. Hiding secret information based on bit technique is so fragile to modification attack. If an attacker change any bit of hidden bits, it is impossible to recover the secret information. In this paper, we proposed a scheme based on Reed- Solomon codes and List Decoding to overcome this problem. We also conduct our solution by analyzing the complexity, security, and experiment.

A traditional barcode is 1-dimension (1D) barcode which only contains data by one side. Quick Response (QR) code is a type of 2-dimension (2D) barcode developed in 1994 by Denso Wave Corporation. QR code got this name because it was developed in order to improve the reading speed of 2D-barcodes. It contains data for both vertical and horizontal dimensions. For this reason, QR code holds a considerably greater volume of information. It can convey various kinds of content such as text, web link, number, and multimedia data. The decoding speed of the QR Code can be 20 times faster than that of other 2D symbols [6]. In recent years, QR code is becoming popular in business via QR readers and mobile devices. Since QR code is so popular, some secret information could be transferred via it. The authors [2], [3], [4] analyzed the

properties of each QR code before embedding it into this one. If they want to embed a secret message into QR code, they will encode it first. After that, they exploit the structure of QR code

which code they want to use. It takes time, risks, and cannot get the secret message directly from this QR code. Lin et al. [1] observed and proposed a novel scheme to solve this problem. The idea to hide secret messages into QR code is to use the error correction capability. This idea is first proposed by Lin et al. [1]. First of all, they encode the secret message *sm* by using a shared key *K* and get *EK*(*sm*). After that, they embed each bit of *EK*(*sm*) into QR code. Their first drawback is that if any bit of *EK*(*sm*) is damaged, it is impossible to recover *sm* from QR code. The second drawback is that if an attacker does not change any bit of *EK*(*sm*) but adds some extra error values into QR code, they cannot recover their secret message. To the best of our knowledge, all previous techniques used bit embedding scheme to embed secret messages into QR code. It is so vulnerable to the modification attack, i.e. an attacker changes any bit of secret messages. We propose using Reed-Solomon code and List Decoding to overcome this kind

of attack.

In Coding Theory, List Decoding, a research field aims to correct as many errors as possible in noisy channels, is rapidly developed in recent years. Peter Elias [14] and M.J. Wozencraft [15] described List Decoding in order to correct errors over noisy channel. Nowadays, it can be found in many applications. It can be used to trace who traitor is [18], [17]. Our contribution: Our main contributions is to propose algorithms that hide a secret message into QR code. The secret message is invisible to attackers and secure against modification or damage attack. We analyze them under complexity and security aspects, and conduct these algorithms by experiments. Outline of the paper: The rest of this paper is organized as the following. Section II presents the preliminaries. Section III describes our proposed solution. The next section describes the security, effectiveness, and testing of our solution. Section V presents experimental results. The last section summarizes the key points and mentions future work.

**Document Authentication Using Graphical Codes: Impacts of the Channel Model:**

This paper proposes to investigate the impact of the channel model for authentication systems based on codes that are corrupted by a physically unclonable noise such as the one emitted by a printing process. The core of such a system is the comparison for the receiver between an original binary code, an original corrupted code and a copy of the original code. We analyze two strategies, depending on whether or not the receiver use a binary version of its observation to

perform its authentication test. By deriving the optimal test within a Neyman-Pearson setup, a theoretical analysis shows that a thresholding of the code induces a loss of performance. This study also highlights the fact that the probability of the type I and type II errors can be better approximated, by several orders of magnitude, computing Chernoff bounds instead of the Gaussian approximation. Finally we evaluate the impact of an uncertainty for the receiver on the opponent channel and show that the authentication is still possible whenever the receiver can observe forged codes and uses them to estimate the parameters of the model.

Authentication of physical products such as documents, goods, drugs, jewels, is a major concern in a world of global exchanges. According to the Organization for Economic Co- operation and Development (OECD), international trade in counterfeit and pirated goods reached more than US $250 billion in 2009 [10], additionally the World Health Orga- nization in 2005 claimed that nearly 25% of medicines in developing countries are forgeries [9]. One way to perform authentication of physical products is to rely on the stochastic structure of the material that

composes the product. Authentication can be performed for example by recording the random patterns of the fiber of a paper [6], but such a system is practically heavy to deploy since each product needs to be linked to its high def- inition capture stored in a database. Another solution is to rely on the degradation induced by the interaction between the product and a physical process such as printing, mark- ing, embossing, carving ... Because of both the defaults of the physical process and the stochastic nature of the mater, this interaction can be considered as a Physically Unclon- able Function (PUF) [12] that cannot be reproduced by the forger and can consequently be used to perform authentica- tion. In [5], the authors measure the degradation of the inks within printed color-tiles, and use discrepancy between the statistics of the authentic and print-and-scan tiles to per- form authentication. Other marking techniques can also be used, in [11] the authors propose to characterize the ran- dom profiles of laser marks on materials such as metals (the

technique is called LPUF for Laser-written PUF) and to use them as authentication features.

We study in this paper an authentication system which uses the fact that a printing process at very high resolution can be seen as a stochastic process due to the nature of differ-ent elements such as the paper fibers, the ink heterogeneity, or the dot addressability of the printer. Such an authenti-cation system has been proposed by Picard et al. [8, 7] and uses 2D pseudo random binary codes that are printed at the native resolution of the printer (2400 dpi on a standard off-

set printer or 812 dpi on digital HP Indigo printer). The whole system is depicted on Fig. 1: once printed on a pack- age to be authenticated, the degraded code can be scanned and thresholded by an opponent (the forger). Note that at this stage the thresholding is necessary because the indus-

trial printers can only print dots, e.g. binary versions of the scanned code. The opponent will produce a printed copy of the original code to manufacture his forgery and the receiver will compare the scanned (and potentially post-processed) version of the original code with the scanned (and poten-tially post-processed) version of the copied code in order to perform authentication. One advantage of this system over previously cited ones is that it is easy to deploy since the au-thentication process needs only a scan of the graphical code under scrutiny and the seed used to generate the original one, no fingerprint database is required.

The security of this system solely relies on the use of a PUF, i.e. the impossibility for the opponent to accurately estimate the original binary code. Different security analysis have already been performed w.r.t. this authentication system, or to very similar ones. In [1], the authors have studied the impact of multiple printed observations of same graphical codes and the authors have shown that the power of the noise due to the printing process can be reduced in this particular setup. In [3], the authors use machine learning tools in order to try to infer the original code from an observation of the printed code, their study shows that the estimation accuracy can be increased without recovering perfectly the original code. In [2], the authors consider the security analysis in the rather similar setup of passive fingerprinting using binary fingerprints under informed attacks (the channel between the original code and the copied code is assumed to be

a Binary Symmetric Channel), they show that the security increase with the code length and they propose a practical threshold when type I error (original detected as a forgery) and type II error (forgery detected as an original) are equal. The goal of this paper is to analyze what are the different strategies for the receiver with respect to the post-processing step. We assume that the strategy of the opponent is fixed and that the copied binary code suffers a binary input binary

output channel. We show that it is in the receiver’s interest to process directly the scanned grayscale code instead of a binary version and we evaluate the impact of the Gaussian approximation of the test with respect to its asymptotic ex- pression. We also investigate the impact of the estimation of the opponent printing channel over the authentication performances.

**Unsynchronized 4D Barcodes Coding and Decoding Time-Multiplexed 2D Colorcodes:**

We present a novel technique for optical data transfer between public displays and mobile devices based on unsynchronized 4D barcodes. We assume that no direct (electromagnetic or other) connection between the devices can exist. Time-multiplexed, 2D color barcodes are displayed on screens and recorded with camera equipped mobile phones. This allows to transmit information optically between both devices. Our approach maximizes the data throughput and the robustness of the barcode recognition, while no immediate synchronization exists. Although the transfer rate is much smaller than it can be achieved with electromagnetic techniques (e.g., Bluetooth or WiFi), we envision to apply such a technique wherever no direct connection is available. 4D barcodes can, for instance, be integrated into public web-pages, movie sequences,

advertisement presentations or information displays, and they encode and transmit more information than possible with single 2D or 3D barcodes.

Encoding and decoding digital information into printed two dimensional bar- codes becomes more and more popular. They are used in advertisements, on business cards or e-tickets, or for referencing to web-pages as in Semapedia (www.semapedia.org). The amount of information that can be decoded robustly from a 2D barcode with ordinary mobile devices, such as mobile phones, is usually restricted to several characters only. Thus, usually IDs, URLs or simple

addresses are encoded. Yet, professional industrial scanners are able to decode a much larger amount of characters (several thousands) with an acceptable reliability. In this paper we present a new kind of barcode that we refer to as 4D barcode. It encodes data in four dimensions: width, height, color and time. Con- sequently, it cannot be printed on paper but is displayed on screens of mobile or spatial devices. Time-multiplexing colored 2D barcodes allows to transmit a larger amount of information robustly to o\_-the-shelf mobile phones without requiring an explicit synchronization.

A large number of applications for mobile phones exist that read and decode printed QR-codes [1] as a standardized black-and-white 2D barcode. Datamatrix [2] is a similar example (yet not as common as QR-codes) and is used by applications like Semacode (www.semacode.com). As mentioned earlier, only a small amount of information can be decoded robustly with consumer camera phones - limiting QR-code or Datamatrix barcodes to encode a few characters only. Han et al. [3] propose Colorcode, a 3D barcode which -in addition to a 2D matrix layout- uses colored bits as third dimension. But due to its small resolution of 5x5 cells it encodes only IDs that are resolved through a central lookup service (www.colorzip.co.jp). Besides applications in advertisement, the Colorcode is used for context aware systems [4]. 2D barcodes have also been

applied to realize interaction techniques with mobile phones. Rohs [5] describes a barcode named Visual Code that stores up to 83 bits of data. Displaying it on a screen, it is used for tracking the movement and rotation of the phone relative to the screen [6, 7]. Another novel approach is presented by Scott et al. [8], who use Spotcode (a circular 2D barcode) for out-of-band device discovery and service selection - bypassing the standard Bluetooth in-band device discovery. This is applied by Madhavapeddy et al. [9] to also implement interaction techniques with Spotcodes that are displayed on a screen - using an online Blue- tooth connection for data exchange. Similar techniques that apply displayed 2D barcodes for supporting mobile phone based interaction methods in combination with screens can be found in [10{12]. Besides barcodes, other possibilities for optical data transfer exist. Shen et al. [13], for example, explain how to read 7-segment digits from LCD/LED displays with camera equipped mobile phones. This system was mainly developed to support people with vision disorders by using their phones to recognize and read the digits on simple displays, such as on clocks. The system requires approximately 3 two seconds for capturing and reading the digits on a Nokia 6630 - which is

comparable to other OCR Software for mobile phones. Yet another interesting new approach for transmitting data optically is to use light sources instead of displays. In visible light communication, ordinary light sources are modulated with a digital signal. Approaches presented by Tanaka et al. [14] or Komine and Nakagawa [15] use white-light LEDs for illuminating a room and for transmit- ting time-multiplexed signals. The modulation frequency is high enough so that the transmitted signal remains invisible to the human eye. The embedded signal is received by photo diodes and is \_nally decoded. Using such a system, it is possible to transmit up to 100 Mbit/s and more.

**Distortion Modeling and Invariant Extraction for Digital Image Print-and-Scan Process:**

After an image is printed-and-scanned, it is usually filtered, rotated, scaled, cropped, contrast-andluminance adjusted, as well as distorted by noises. This paper presents models for the print-and-scan process, considering both pixel value distortion and geometric distortion. We show properties of the discretized, rescanned image in both the spatial and frequency domains, then further analyze the changes in the Discrete Fourier Transform (DFT) coefficients. Based on these properties, we show several techniques for extracting invariants from the original and rescanned image, with potential applications in image watermarking and authentication. Preliminary

experiments show the validity of the proposed model and the robustness of the invariants.

Today the print-and-scan (PS) process is commonly used for image reproduction and distribution. It is popular to transform images between the electronic digital format and the printed format. The rescanned image may look similar to the original, but may have been distorted during the process. For some image security applications, such as watermarking for copyright protection, users should be able to detect the embedded watermark even if it is

printed-and-scanned. In image authentication cases, the rescanned image may be considered as authentic, because it is a reproduction of the original. Little work has been done to understand the changes that digital images undergo after the PS process. Most work discusses individual models of printing or scanning. In this paper, we begin with the characteristics of the PS process. Then, in Section 3, we propose a model that can be used to analyze the distortion of a discretized digital image after the PS process in the spatial and frequency domain. Then, we will analyze the variations of DFT coefficients, leading to important properties for extracting invariants. In Section 4, we discuss several methods that can be used to extract invariants of the PS process. Some experimental results, including an analysis of the feature vector proposed in [5], are shown in Section 5. In Section 6, we make a summary and discuss some future work.

Distortion occurs in both the pixel values and the geometric boundary of the rescanned image. The distortion of pixel values is caused by (1) the luminance, contrast, gamma correction and chromnance variations, and (2) the blurring of adjacent pixels. These are typical effects of the printer and scanner, and while they are perceptible to the human eye, they affect the visual

quality of a rescanned image. Distortion of the geometric boundary in the PS process is caused by rotation, scaling, and cropping (RSC). Although it does not introduce significant effects

on the visual quality, it may introduce considerable changes at the signal level, especially on the DFT coefficients of the rescanned image. It should be noted that, in general image editing

processes, geometric distortion cannot be adequately modeled by the well-known rotation, scaling, and translation (RST) effects, because of the design of today’s Graphic User Interface (GUI) for the scanning process. From Figure 1, we can see that users can arbitrarily select

a range for the scanned image. We use “cropping” to describe this operation, because the rescanned images are cropped from an area in the preview window, including the printed image and background. The RST model, which has been widely used in pattern recognition, is

usually used to model the geometric distortion on the image of an observed object. In those cases, the meaning of RST is based on a fixed window size, which is usually pre-determined by the system. However, in the PS process, the scanned image may cover part of the original

picture and/or part of the background, and may have an arbitrarily cropped size. These changes, especially that of image size, will introduce significant changes of the DFT coefficients. Therefore, instead of RST, a RSC model is more appropriate to represent the PS process.

**SURVEY ON INFORMATION HIDING TECHNIQUES USING QR BARCODE:**

Nowadays, the information processing system plays crucial part in the internet. Online information security has become the top priority in all sectors. Failing to provide online

information security may cause loss of critical information or someone may use or distribute

such information for malicious purpose. Recently QR barcodes have been used as an effective

way to securely share information. This paper presents the survey on information hiding

techniques which can share high security information over network using QR barcode.

Due to tremendous growth in communication technology, sharing the information through the

communication network has never been so convenient. Nowadays information is processed

electronically and conveyed through public networks. Such networks are unsecured and hence

sensitive information needs to be protected by some means. Cryptography is the study of

techniques that allows us to do this. In order to protect information from various computer attacks as well as network attacks various cryptographic protocols and firewalls are used. But no single measure can ensure complete security.

Nowadays, the use of internet and sharing information are growing increasingly across the globe,

security becomes a vital issue for the society. Security attacks are classified as passive attacks and active attacks [11, 12]. In passive attacks, attacker monitors network traffic and looks for

sensitive information but does not affect system resources. Passive attacks include traffic analysis, eavesdropping, Release of message contents [11, 12]. In active attack, attacker breaks

protection features to gain unauthorized access to steal or modify information. Active attacks

include masquerade, replay, modification of messages, and denial of service [11, 12].Therefore,

security threats (such as eavesdropping, data modification, phishing, website leaks etc.) force us

to develop new methods to counter them. Considering QR barcodes as an effective media of

sharing information, many researchers have proposed information/data hiding methods [6,7, 8, 9.] as well as online transaction systems [1,2,3,4,5] using QR barcode. In this paper, we describe

different information hiding schemes using QR barcode