HIGH RATE ROBUST CODES WITH LOW IMPLEMENTATION COMPLEXITY

N.GIRIDHARAN M.E.[1], V.KUMARAVEL[2],

ASSISTANT PROFESSOR[1] ,K.S.RANGASAMY COLLEGE OF TECHNOLOGY, TIRUCHENGODE,TAMILNADU, INDIA

BE STUDENT[2] ,K.S.RANGASAMY COLLEGE OF TECHNOLOGY, TIRUCHENGODE, TAMILNADU, INDIA

ABSTRACT

The quick response Fault Injection Attack Elimination(QRFIE) code was designed for storage information and high-speed reading applications. In this paper, we present a new Read Solomon and four dimensional diffie Hellman algorithm. If a third party listened to the exchange, it would be computationally difficult for them to determine the secret colours. In fact, when using large numbers rather than colours, this action is computationally expensive for modern supercomputers to do in a reasonable amount of time. That has two storage levels and can be used for document authentication. The private level is constructed by replacing the black modules by specific textured patterns.

It consists of information encoded using q-ary code with an error correction capacity. This allows us not only to increase the storage capacity of the QRFIE code, but also to distinguish the original document from a copy. This authentication is due to the sensitivity of the used patterns to the print-and-scan (P&S) process. The pattern recognition method that we use to read the second-level information can be used both in a private message sharing and in an authentication scenario. It is based on maximizing the correlation values between P&S degraded patterns and reference patterns. The storage capacity can be significantly improved by increasing the code alphabet q or by increasing the textured pattern size. The experimental results show a perfect restoration of private information. It also highlights the possibility of using this new rich QRFIE code for document authentication.

1 INTRODUCTION

1.1 QRFIE CODE MANAGEMENT:

Today graphical codes, such as EAN-13 barcode, Quick response Fault Injection Attack Elimination(QRFIE) code, Data Matrix , PDF417, are frequently used in our daily lives. These codes have a huge number of applications including: information storage (advertising, museum art description), redirection to web sites, track and trace (for transportation tickets or brands), identification (flight passenger information, supermarket products) etc. The popularity of these codes is mainly due to the following features: they are robust to the copying process, easy to read by any device and any user, they have a high encoding capacity enhanced by error correction facilities, they have a small size and are robust to geometrical distortions. However, those undeniable advantages also have their counterparts:

1) Information encoded in a QRFIE code is always accessible to everyone, even if it is ciphered and therefore is only legible to authorized users (the difference between “see” and “understand”).

2) It is impossible to distinguish an originally printed QRFIE code from its copy due to their insensitivity to the Print-and-Scan (P&S) process.

2 LITERATURE REVIEW

2.1 CODING AND DECODING IN QRFIE CODES

Commonly the characters, numbers etc are embedding in QRFIE codes. This paper introduces the concept of color image embeddings in QRFIE codes. This is an automatic method to embed QRFIE codes into color images with bounded probability of detection error. These embeddings are compatible with standard decoding applications and can be applied to any color image with full area coverage. To mitigate the visual distortion of the QRFIE image, the algorithm utilizes halftoning masks for the selection of modified pixels and nonlinear programming techniques to locally optimize luminance levels take one color image and converted into gray image. Then this doing the masking process, window extraction, image embedding, decoding like processes. After this process the original gray image is taken from this.

we propose to overcome these shortcomings by enriching the standard QRFIE code encoding capacity. This enrichment is obtained by replacing its black modules by specific textured patterns. Besides the gain of storage capacity, these patterns can be designed to be sensitive to distortions due to the P&S process. These patterns, that do not introduce disruption in the standard reading process, are always perceived as black modules by any QRFIE code reader. Therefore, even when the private information is degraded or lost in the copy, the public information is always accessible for reading. The proposed two level QRFIE (4LQRFIE) code contains of: a first level accessible for any standard QRFIE code reader, therefore it keeps the strong characteristics of the QRFIE code; and a second level that improves the capacities and characteristics of the initial QRFIE code. The information in the second level is encoded by using $q-$ary ($q \geq 2$) code with error correction capacities.

This information is invisible to the standard QRFIE code reader because it perceives the textured patterns as black modules. Therefore, the second level can be used for private message sharing. Additionally, thanks to textured pattern sensitivity to P&S distortions, the second level can be used to distinguish the original 4LQRFIE code from its copies.

2.2 2D BAR-CODES FOR AUTHENTICATION

In this work, we investigate the authentication problem of real-world goods on which 2D bar-codes (2D-BC) were printed and we take the opponent’s point of view. The opponent is assumed to have access to Nc noisy copies of a genuine 2D-BC (noise being due to printing and scanning processes). A simple estimator of the 2D-BC based on copies averages is proposed, letting the opponent print a fake 2DBCwhich aims at being declared as genuine by the system detector. Performance of the estimator in terms of error probability at the detector side is then derived with respect to Nc and compared with experimental results on real 2D-BC. It is shown that the opponent can produce a fake that successfully fools the detector with a reasonable number of genuine goods.

When making sure a real-world good (such as medicine, wine, textile,) is genuine, 2D bar-codes (2D-BCs) area n alternative to watermarks. 2D-BCs [2] (also called Data Matrix or Data Grid) are black-and-white visible images encoding a good binary identifier using a (secret) cryptographic key in a pseudo-random way and printed on the goods package. Using an automated detection process based on a scan of the 2D-BC, a correlation score is computed and compared to a pre-determined threshold in order to decide whether the good is genuine or fake.

In this context, an opponent (Eve) aims at producing a fake 2D-BCs declared as genuine by the detector, whereas the goal of the product manufacturer (Bob) is to make such are production difficult or impossible for Eve. Bob will therefore use the production process noises all the more severe as the printed 2D-BCs size is small (around 4 milli meters).He might even deliberately add some noise during his 2DBCprinting process to obtain properties similar to Physical Unclonable Functions. Besides, Eve, unaware of the good binary identifier encoding, has no choice but to try to estimate the original 2D-BC without getting to the good identifier.

2.3 TWO LEVEL QRFIE CODE

The Quick response Fault Injection Attack Elimination(QRFIE) code was designed for storing information. These codes have a huge number of applications including: in format ion storage (advertising, museum art description), redirection to web sites, track and trace (for transportation tickets or brands), identification (flight passenger information, supermarket products) etc. In our proposed system the new rich QRFIE code there are two storage levels and can be used for document authentication. This new rich QRFIE code, named two levels QRFIE code (2LQRFIE), has public and private storage levels. The public level is the same as the standard QRFIE code storage levels; therefore it is readable by any classical QRFIE code application. The private level is code with an error correction capacity. The pattern recognition method is used to read the second level information and be used both in a private message sharing scenario. The experimental results show a perfect restoration of private information. It also highlights the possibility of using this new rich QRFIE code for document authentication.

The QRFIE code generation algorithm consists of information encoding using Reed-Solomon error correction code, information division on codewords, application of mask pat tern, placement of codewords and function patterns into the QRFIE code. The QRFIE code recognition algorithm includes the scanning process, image binarization, geometrical correct ion and decoding algorithm. The simplest type of rich QRFIE codes is the user-friendly QRFIE code. The target of these codes is to improve the aesthetic view of QRFIE codes. It consists of changing the colors and shape of the modules, or of adding an image into the QRFIE code. Different design QRFIE code generators are proposed as free or paid applications.2 However, most of these generators prefer to sacrifice the possibility of error correction for attractive design. Recently, the rich QRFIE code, which adds the significance without losing error correction capacity, was introduced in [3]. The authors proposed a novel method of blending a color image into the QRFIE code, which modifies the QRFIE code source pixels so that the white (rsp. black) module pixels are transformed from white (rsp. black) to any RGB values and whose luminance value is considered as white (rsp. black) pixel by QRFIE code binarization method. Recently, the QRFIE code steganography, which aims to hide a secret message into a QRFIE code, was introduced. In [4] and [5] the authors suggest inserting the secret message by using the error correction capacity of the QRFIE code. That means, they changed the bits encoded in the standard QRFIE code, and inserted errors into it. In this case, the secret message does not disturb the reading process of the QRFIE code message, but the error capacity of QRFIE code is low.

3 PROPOSED SYSTEM

The proposed 4 dimensional QRFIE code depends on the textured pattern size, the alphabet dimension *q* and the textured pattern density. For example, if we want to increase the storage capacity of the 4LQRFIE code (either by decreasing the pattern size or increasing the alphabet dimension), the robustness (pattern recognition rate) will decrease (significantly or not). Analogically, the boundary values of textured pattern densities (significantly low or high) decrease the 4LQRFIE code robustness. Therefore, we should take into account two trade-offs: storage capacity- robustness trade-off and QRFIE code contrast – robustness trade-off.

The QRFIE code generation algorithm consists of information encoding using Reed-Solomon error correction code, information division on codewords, application of mask pattern, placement of codewords and function patterns into the QRFIE code. The QRFIE code recognition algorithm includes the scanning process, image binarization, geometrical correction and decoding algorithm

4 RESULTS AND DISCUSSION

Classic coding theory addresses the problem of reliability of information transmitted over a noisy channel or stored in storage media. In classic coding theory, the errors are assumed to be random and the probability that the channel will introduce an error is relatively small. Consequently, a reliability oriented code should protect the system from random errors of small multiplicity. Many of the known codes designed for reliability (such as the parity bit code, the RM code, the Hamming code, cyclic codes, BCH codes, etc) are linear . In linear codes, all the errors that are codewords are never detected. As a result, reliability oriented codes cannot be used to provide security against an attacker

5 CONCLUSION

In this project, reducing labour cost technology. The recognition of new font characters by the system is very easy and quick. If can reuse the edited information as and when required. The extension to software other than editing and searching is topic for future works. The Grid infrastructure used in the implementation of Optical Character Recognition system can be efficiently used to speed up the translation of image based documents into structured documents that are currently easy to discover, search and process.

Our algorithm successfully detects the Signature Details region from the image which consists of User Document number & then character segmentation, recognition .User have applied our algorithm on many images and found that it successfully recognition. The project was designed keeping in mind the automation of the Signature Details detection system for security reason that could replace the current system of manual entry.

6 REFERENCES

1. T. G. Zimmerman, G. F. Russell, A. Heilper, B. A. Smith, J. Hu, D. Markman, J. E. Graham, C. Drews, Retail Applications of Signature Verification, Proceedings of SPIE2004, Volume 5404, Biometric Technology for Human Identification, Anil K. Jain, Nalini K. Ratha, Editors, 206-214, August 2004.

2. J. Richiardi, J. Fierrez-Aguilar, J. Ortega-Garcia, A. Drygajlo, On-Line Signature Verification Resilience to Packet Loss in IP Networks, Proc. 2nd COST 275 Workshop on Biometrics on the Internet: fundamentals, advances and applications, 9-14, 2004

3. S. N. Srihari, A. Xu, and M. K. Kalera, Learning Strategies and Classification Methods for OffLine Signature Verification, 9th Int. Workshop on Frontiers in Handwriting Recognition (IWFHR’04), 161-166, 2004