



e-ISSN: 2319-8753 | p-ISSN: 2320-6710

# IJIRSET

International Journal of Innovative Research in  
**SCIENCE | ENGINEERING | TECHNOLOGY**

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 5, May 2021

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 7.512**

9940 572 462

6381 907 438

[ijirset@gmail.com](mailto:ijirset@gmail.com)

[www.ijirset.com](http://www.ijirset.com)

# Two Level QRFIE Code for Private Message Sharing

S.Ponni<sup>1</sup>, J.Ananthi<sup>2</sup>, S.Priyadharshini<sup>2</sup>, D.Savitha<sup>2</sup>

Assistant Professor, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode, Tamilnadu, India<sup>1</sup>

UG Students, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode, Tamilnadu, India<sup>2</sup>

**ABSTRACT:** The QR code is widely popular in daily due to reading high speed application and greater storage capacity of storing information. The objective of the paper is to use a QR code for hiding private message sharing. If any unauthorized person is able to access a private message in different ways, they can't be able to access because it will be difficult for them to determine the secrets colors. The private level is designed by replacing the modules using specific textured patterns. This allows not only to increase the storage capacity but also to improve the security of QR code. The main purpose of a private message sharing scenario is the invisible storage and transmission of private information into QR code. In this project, a new reed Solomon and four dimensional Diffie Hellman algorithm is introduced. It proposes a genetic technique to detect and react to fault attacks on embedded software. From the analysis, the security level is increased while sharing the private message.

**KEYWORDS:** FAME-QR code, Diffie Hellman, Fault attacks, Pattern recognition, Two storage levels.

## I. INTRODUCTION

### A. FAULT ATTACKS MANAGEMENT

Today graphical codes, such as EAN-13 barcode, Fault Aware Microprocessor Extension Quick response (FAME-QR) code, Data Matrix, PDF417, are frequently used in our daily lives. FAME-QR codes have a large number of applications including redirection to web sites, track and trace (for transportation tickets or brands), identification (flight passenger information, supermarket products), information storage (advertising, museum art description), etc. However, those undeniable advantages also have their counterparts:

- 1) Information encoded in a FAME-QR code is always accessible to everyone, even if it is ciphered and therefore is only legible to authorized users
- 2) It is impossible to differentiate an originally printed FAME-QR code from its copy due to their insensitivity to the Print-and-Scan (P&S) process.

The proposed two levels FAME-QR (4LFAME-QR) code contains of: a first level accessible for any standard FAME-QR code reader, therefore it keeps the strong characteristics of the FAME-QR code; and a second level that improves the capacities and characteristics of the initial FAME-QR 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 FAME-QR code reader because it perceives the textured patterns as black modules. Therefore, private message sharing is done in second level. Additionally, thanks to textured pattern sensitivity to P&S distortions, the second level can be used to distinguish the original 4LFAME-QR code from its copies.

### B. FAULT ATTACK MITIGATION

Nowadays, the increasing complexity and robustness of digital systems have a significant impact on dependability and diagnostic features of these systems. From various platforms which are currently used for implementation of these system based on the SRAM-based Field Programmable Gate Arrays (FPGAs) which is one of

the most frequently used hardware. FPGAs are becoming increasingly popular for many applications due to their high-throughput capabilities and relatively low cost. On the other hand, SRAM based FPGAs are unsafe to radiation effects such as Single Event Upset (SEU) which cause the change in the state of a digital memory element and the function implemented in FPGA can cause unacceptable change. Therefore, reliable implementation techniques that can repair and migrate these SEU effects are desirable. There were many techniques present for identifying the appeared fault. The technique of mitigation usually involves several steps: error detection during system operation for which Concurrent Error Detection (CED) techniques can be used, fast fault localization (e.g. on-line checkers) and quick recovery from failures (e.g. reconfiguration of a FPGA chip).

### C. EMBEDDED SOFTWARE

This research investigates fault attacks on embedded software, which is a powerful hardware-oriented implementation attack against security mechanisms implemented in software running on modern embedded devices. In a fault attack on embedded software, the target of the fault injection is the hardware layer while the target of the fault exploitation is the software layer. The adversary creates a controlled and engineered fault in the processor hardware, and exploits the effects of the fault on the software to cause sensitive information leakage or to obtain control over the embedded processor. For instance, outlines the process of a typical fault attack on unprotected embedded cryptographic software. In this example, the cryptographic software makes use of a secret key, and the adversary aims to learn the value of this key. The adversary starts with performing fault injection on the hardware, including the microprocessor pipeline, registers, and memory. Fault injection can be achieved by various means such as reducing supply voltage, increasing operating frequency, or increasing ambient temperature of the processor beyond the allowed margins.

### D. MICROARCHITECTURE

MESS is based on an open-source, cycle-accurate, micro-architecture level, full system simulator gem. As, additional fault injection and analysis capabilities are integrated into gem5 to extend it to MESS. The extensions consist of three main components: Trigger Generator, Fault Injector, and Run-time Status Monitor. The Trigger Generator enables a user to define trigger conditions to enable/disable the fault injection. The Fault Injector enables a user to define timing, location, and type of the faults to be injected. It also performs the fault injection based on the defined fault parameters and trigger conditions. The Run-time Status Monitor allows a user to define run-time events to be monitored during the simulation. These events may be used to check if an attack is successful (e.g., bypassing a security check), or to get diagnostic information about fault behaviour of the target program. The inputs of MESS are an executable binary file for the target software, a micro MESS is based on an open-source, cycle-accurate, micro-architecture level, full system simulator gem5. As it is shown in, additional fault injection and analysis capabilities are integrated into gem5 to extend it to MESS. The extensions consist of three main components: Trigger Generator, Fault Injector, and Run-time Status Monitor. The Trigger Generator enables a user to define trigger conditions to enable/disable the fault injection. The Fault Injector enables a user to define timing, location, and type of the faults to be injected. It also performs the fault injection based on the defined fault parameters and trigger conditions. The Run-time Status Monitor allows a user to define run-time events to be monitored during the simulation. These events may be used to check if an attack is successful (e.g., bypassing a security check), or to get diagnostic information about fault behaviour of the target program. The inputs of MESS are an executable binary file for the target software, a micro.

### E. FAULT DETECTION

FAME depends on a hardware fault detection unit (FDU) that may be a set of observers watching processor's operation to detect anomalies. throughout the conventional operation, associate application runs within the nominal mode and no overhead is increased. Upon detection of a fault, FDU asserts associate alarm signal to apprise the processor of a possible fault attack. The detector configuration and sensitivity level of FDU rely on the appliance domain and therefore the assailant model supported needs, FDU is ready to derive the fault standing of the processor by combining differing types and variety of fault detectors. These embrace clock/voltage fault detectors, magnetism pulse detectors, coincident error detection strategies, shadow latches, and error detection codes. The need of the observers utilized in FDU is that they have to detect fault injection before a faulty worth is employed by a sequent instruction. During this work, we have a tendency to observe faults that originate from temporal arrangement violations and localized magnetism pulses. Given the error detection mechanisms enumerated higher than, however, it's clear that FDU mechanism is generic which it will handle a large number of fault detection mechanisms. This section provides

characterization results for the temporal arrangement device of the celebrity example. The characterization results for the EM device may be found in Master Thesis of Chimney Desponded, a member of FAME development team. The sensitivity of the Fault Detection Unit is evaluated by injecting faults with completely different parameters into the fault-resistant ASIC and by checking its response. Specifically, we have a tendency to inject a clock-glitch to violate setup-time and so examine the response of the detection unit.

## F.CHECKPOINTING

For fault-attack-resistant execution of the secure entices mechanism, FAME provides a hardware-level check inform support; the fault response registers (FRR). They embody the status register of the processor, the name and address to the interrupted program, and also the register file inputs of the write back stage. To mitigate the fault attacks, we tend to propose Fault-attack Aware microchip Extensions (FAME) that transforms Associate in Nursing unprotected baseline processor to a fault-attack resistant processor. The most objective of FAME is to supply affordable architectural support for fault mitigation within the processor hardware to modify software system designers to develop cheaper and safer fault attack countermeasures. FAME achieves its objective by distributing fault detection and response across multiple abstraction layers. FAME combines the sturdy points of the previous techniques. The secure entice handler then executes a user-defined fault-response to implement application-specific countermeasures. FAME doesn't suffer from the performance overhead of redundant software system execution, and it responds to a fault injection before its result will spread. Compared to software system redundancy and software system check inform, a hardware sensing element offers low response latency, Associate in Nursing it should modify detection of a fault injection try before an actual fault within the processor happens. the utilization of a sensing element brings a big advantage, as it also reduces the value of the overhead. For embedded or performance sensitive implementations, stripped-down performance overhead is a crucial concern.

## II. RELATED WORK

Commonly the characters, numbers etc. are embedding in FAME-QR codes. Introduces the thought of colour image embedding in FAME-QR codes[1]. This can be associate automatic technique to engraft FAME-QR codes into colour pictures with delimited chance of detection error. These embedding are compatible with commonplace secret writing applications and might be applied to any colour image with full space coverage. To mitigate the visual distortion of the FAME-QR image, the algorithmic rule utilizes 0.5 toning masks for the choice of changed pixels and nonlinear programming techniques to domestically optimize brightness levels Take one colour image and born-again into grey image[1]. Then this doing the masking method, window extraction, image embedding, secret writing like processes. FAME-QR code a sort of two-dimensional barcode investigated by Denso Wave is presently utilized in Japan usually the characters, numbers etc. are embedding in FAME-QR codes.

In this work, It investigates 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[2]. 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 2DBC which aims at being declared as genuine by the system detector. [2] 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 a reproduction 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 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].

The Fault Aware microchip Extension fast response (FAME-QR) code was designed for storing info. These codes have an enormous range of applications including: Informant particle storage, redirection to websites, track and trace, identification. In our projected system the new wealthy FAME-QR code there at 2 storage levels and might be used for document authentication[3]. This new wealthy FAME-QR code, named 2 levels FAME-QR code (2LFAME-QR), has public and personal storage levels. [3] The general public level is that the same because the standard FAME-QR code storage levels; so it's legible by any classical FAME-Code application.[3] The personal level is code with a slip-up correction capability. The pattern recognition methodology is employed to browse the second level info and be used each in an exceedingly personal message sharing situation. The FAME-QR code generation algorithmic rule consists of data cryptography exploitation Reed-Solomon error correction code, info division on code words,

application of mask pattern, placement of code words and performance patterns into the FAME-QR code. The FAME-QR code recognition algorithmic rule includes the scanning method, image closing, geometrical correct particle and secret writing algorithmic rule. It consists of changing the colours and form of the modules, or of adding a picture into the FAME-QR code[3]. The authors projected a unique methodology of mixing a colour image into the FAME-QR code, that modifies the FAME-QR code supply pixels in order that the white module pixels are transformed from white to any RGB prices and whose luminosity value is taken into account as white constituent by FAME-QR code closing methodology.

FAME-QR Codes (2D barcodes) area unit accustomed cipher and rewrite information at a fast rate. Using camera phones to scan 2 dimensional barcodes for a varied function is presently a popular topic in each analysis and in sensible applications. However as yet, the data provided by FAME-QR Codes was alone static. [4] for instance, a public tag can be decoded and translated into “Good evening John Smith” or “Bonjour Jean Depend”, if the system is ready to get information like the name of the user, the language used on the machine (English or French for instance) and therefore the moment once the interaction takes place[4]. Computers area unit widespread and plenty of everyday-objects come back equipped with computer technology. Mobile phones area unit equipped with high-resolution colour displays, wireless access to the web, and respectable process power and memory. Nowadays, different styles of codes area unit employed in order to store retrieve and manage info. He explained: The aim of this paper is to gift discourse FAME-QR Codes: rather than continually exposing identical info to everyone, a contextualized FAME-QR Code is computed in order to supply specific info betting on a specific context.

Verification of document legitimacy may be a current necessary drawback. During this paper we have a tendency to propose to use a rough-textured image containing a visible message, which might be used for identification of variations between written legitimate document and written faux document. The urged rough-textured image consists of specific patterns that ought to satisfy explicit conditions so as to provide smart recognition results when print and Scan (P&S) method. In this work we have a tendency to propose to develop a security pattern to spot the genuineness of a written document. The legitimate supply creates a rough-textured image by writing visible message exploitation n chosen binary patterns happiness to information of known patterns. During verification, the receiver scans the rough-textured image and applies the detection methodology so as to verify the genuineness of rough-textured image (i.e. the structure of P&S patterns corresponds to a structure of original patterns) yet on establish the visual message (i.e. the visual message has got to be legible when pattern detection). During this paper, we have a tendency to propose a rough-textured pattern-based methodology that exploits the actual fact that a forger doesn't have access to the original digital document. This rough-textured image helps the receiver to verify the written document's legitimacy.

In this paper, we have a tendency to upset the planning of high-rate structure two-dimensional (2D) bar codes for the print-and scan channel.[17] Firstly, we have a tendency to derive Associate in nursing boundary on the most achievable rate of those codes by finding out Associate in Nursing inter-symbol interference (ISI) free, perfectly synchronized, and quiet print-and-scan channel, during which the printer device uses 0.5 toning to simulate multiple grey levels. Secondly, we have a tendency to in brief review 3 progressive coded modulation techniques for the additive white Gaussian noise channel (AWGN) within the high quantitative relation signal/noise ratio signal/noises' Narration (SNR) ratio regime, namely, structure secret writing with period coding (MLC/MSD), structure secret writing with parallel freelance coding (MLC/PID), and bit interleaved coded modulation (BICM). [17] Thirdly, we have a tendency to gift a replacement model of the print-and-scan channel specifically tailored to the structure 2nd Universal Product Code application. Two-dimensional bar codes at terribly engaging for varied applications, where a significant quantity of information must be hold on onto paper, plastic or alternative data carriers. Another engaging characteristic of 2nd bar codes as data storage modules consists in their low price: low-cost printer and reader devices exist for the foremost common media.[17] For example, optical device or inkjet halftone printers will be used for printing on paper; optical device engraving, a cheap and prime quality technique, will be used for printing on plastic; moreover, cheap and low-resolution charged coupled device (CCD) primarily based scanners or digital cameras, like those present in cell phones, will be used for reading the written data.

### III. EXISTING SYSTEM

In existing FAME-QR code encodes the information into binary form. Each information bit is represented by a black or a white module. The 2 Dimensional Reed-Solomon error correction code is used for data encryption. Therefore, one



of 4 error correction levels has to be chosen during FAME-QR code generation. The certification of FAME-QR code was performed by International Organization of Standardization (ISO) three position tags are used for FAME-QR code detection and orientation correction. One or more alignment patterns are used to code deformation adjustment. The module coordinates are set by timing patterns. Furthermore, the format information areas contain error correction level and mask pattern. The code version and error correction bits are stored in the version information areas.

#### IV. PROPOSED SYSTEM

The proposed 4 dimensional FAME-QR 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 4 L FAME-QR 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 4LFAME-QR code robustness. Therefore, we should take into account two trades-offs: storage capacity-robustness trade-off and FAME-QR code contrast – robustness trade-off. The FAME-QR code generation algorithm consists of information encoding using Reed-Solomon error correction code, information division on code words, application of mask pattern, placement of code words and function patterns into the FAME-QR code. The FAME-QR code recognition algorithm includes the scanning process, image finalization, geometrical correction and decoding algorithm.

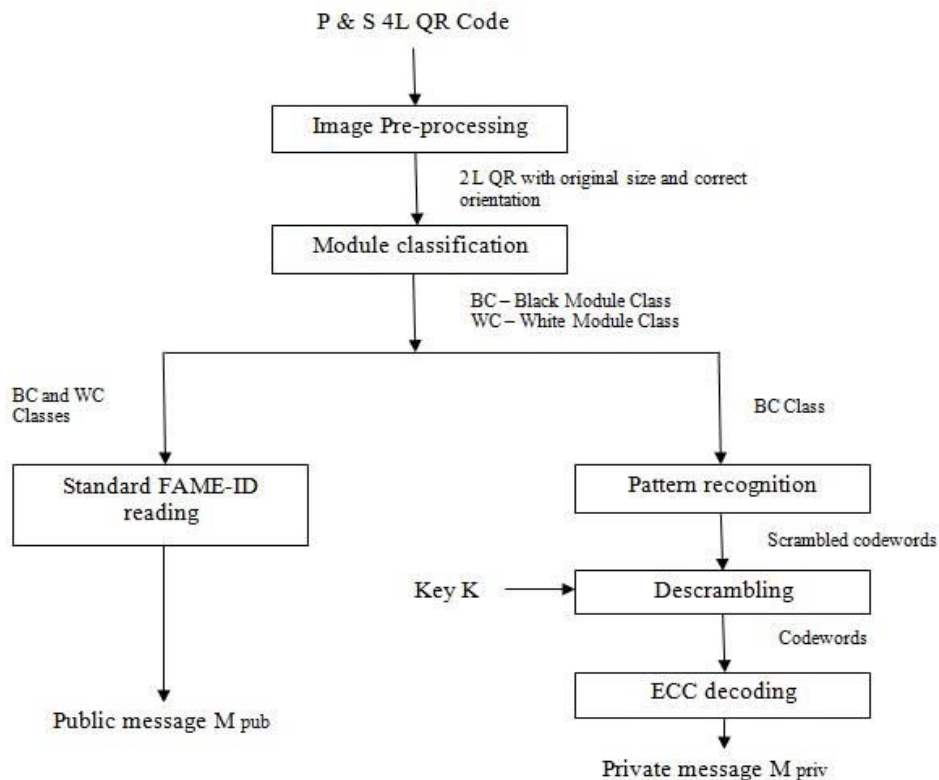


Figure 1. Architecture Diagram

V. EXPERIMENTAL RESULTS

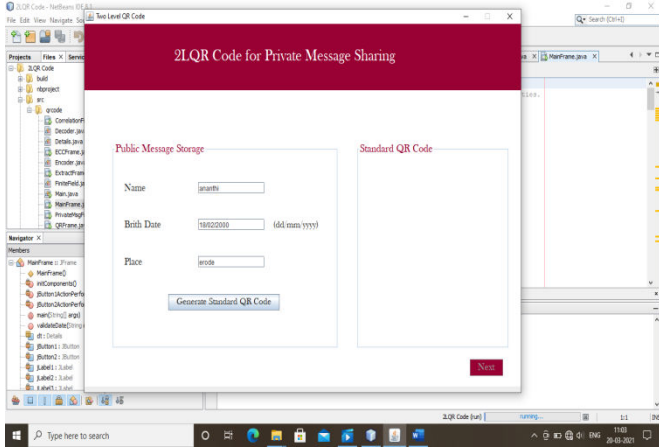


Figure 2. User Details

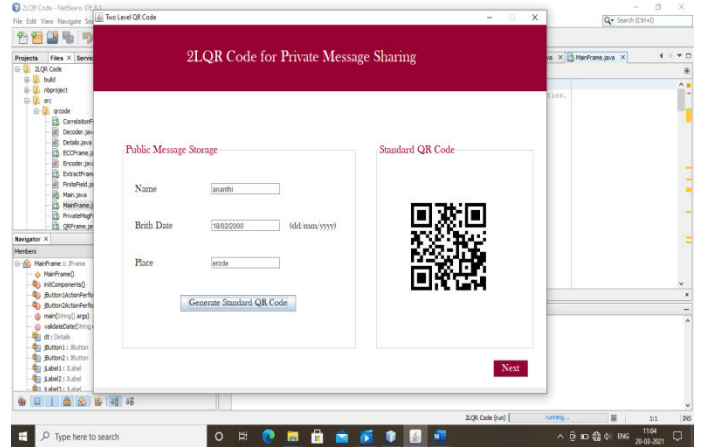


Figure 3. Generating QR code

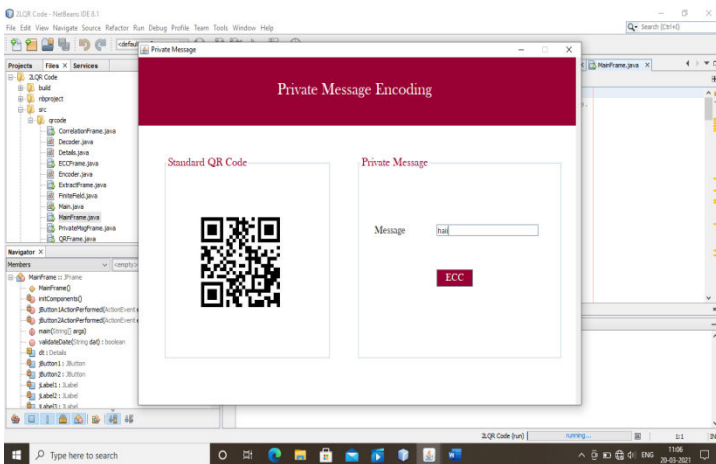


Figure 4. Entering Private Message

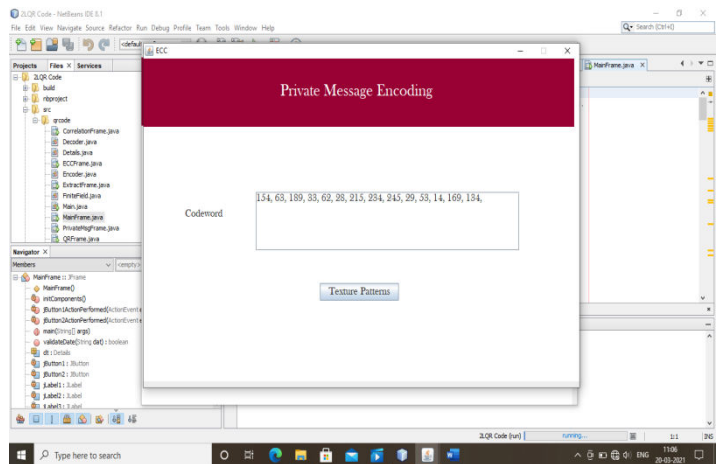


Figure 5. Pattern Recognition

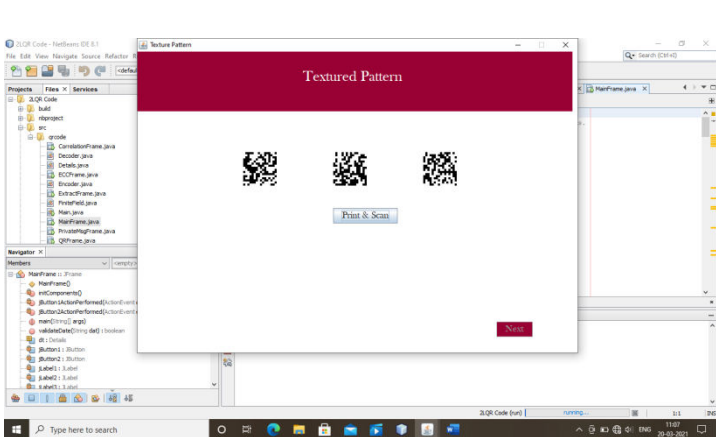


Figure 7. Coloured Textured Patterns

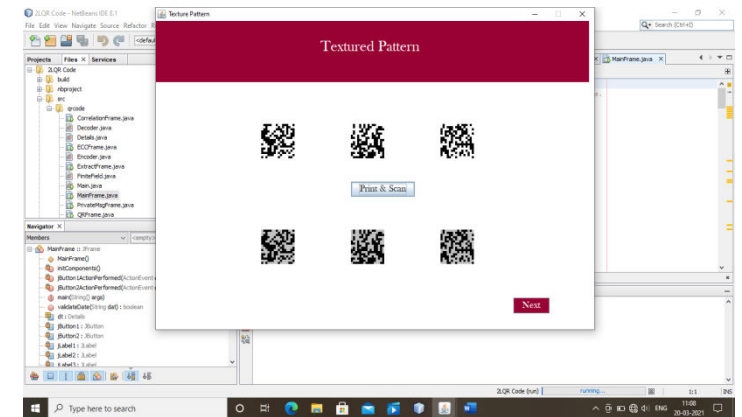


Figure 6. Textured Patterns

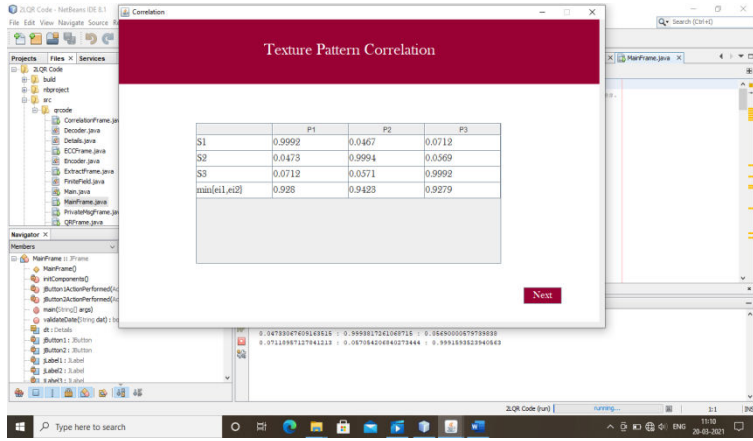


Figure 8. Texture Pattern Correlation

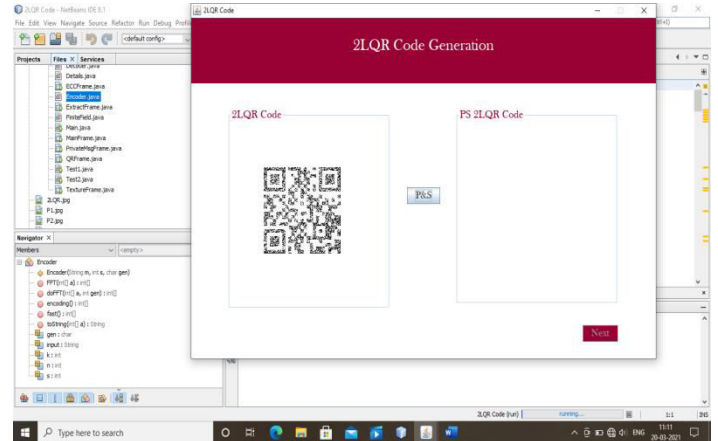


Figure 9. 2L QR Code Generation

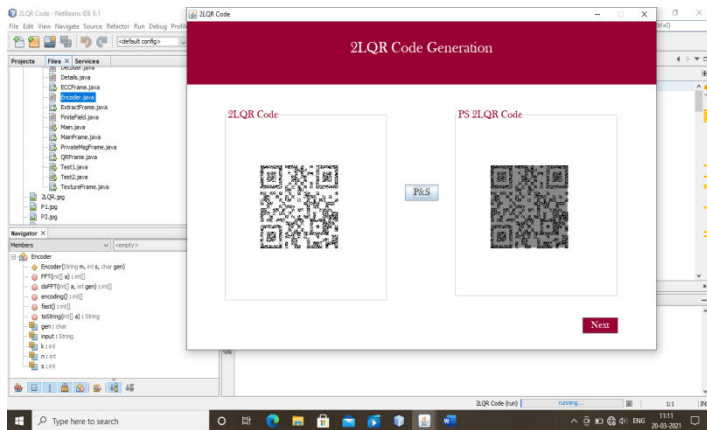


Figure 10. PS 2L QR Code

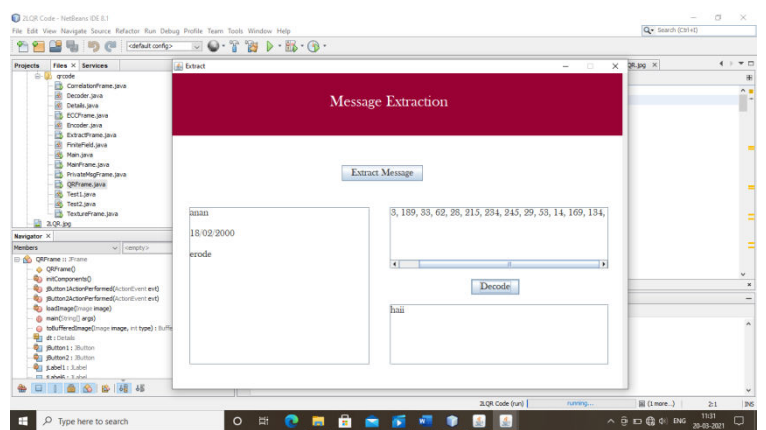


Figure 11. Secret Message Extraction

VI. CONCLUSION

The private level is created by replacing black modules with specific textured patterns. These textured patterns are considered as black modules by standard FAME-QR code reader. Thus the private level is invisible to standard FAME-QR code readers. In addition, the private level does not affect in anyway the reading process of the public level. The proposed 2LFAME-QR code increases the storage capacity of the classical FAME-QR code due to its supplementary reading level. The storage capacity of the 2LFAME-QR code can be improved by increasing the number of textured patterns used or by decreasing the textured pattern size. It is possible to obtain good pattern recognition results, and therefore a successful private message extraction. However, we are facing a trade-off between the pattern size, the alphabet dimensions and the quantity of stored information during the 2LFAME-QR code generation. The suggested textured patterns can be distinguished only after one P&S process. Therefore, we can use the detection method with original patterns in order to ensure good document authentication results.





#### REFERENCES

- [1] T. Langlotz and O. Bimber, "Coding and decoding in fault attacks", Proc. 3rd Int. Symp., ISVC 2014, Lake Tahoe, NV, USA, Nov. 26–28, 2019, pp. 363–374.
- [2] C.-Y. Lin and S.-F. Chang, "2D bar-codes for authentication", Proc. Int. Symp. Multimedia Inf. Process, 2017, pp. 1–10.
- [3] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, "Two Level Fault Attacks", Proc. IEEE Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS), Dec. 2015, pp. 22–25
- [4] Information Technology—Automatic Identification and Data Capture Techniques—Bar Code Symbology—FAME-QR Code, ISO/IEC Standard 18004:2000, 2000.
- [5] Z. Baharav and R. Kakarala, "Visually Significant FAME-QR Codes: Image Blending and Statistical Analysis", Proc. IEEE Int. Conf. Multimedia Expo (ICME), Jul. 2013, pp. 1–6.
- [6] C. Baras and F. Cayre, "2D Bar-Codes For Authentication: A Security Approach", Proc. 20th Eur. Signal Process. Conf. (EUSIPCO), Aug. 2012, pp. 1760–1766.
- [7] T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, "Robust message hiding for FAME-QR code" , IEEE Proceedings, 10th International Conference Intell. Inf. Hiding Multimedia Signal Process. (IIH MSP), Aug. 2014, pp. 520–523.
- [8] A. T. P. Ho, B. A. M. Hoang, W. Sawaya, and P. Bas, "Document authentication using graphical codes: Reliable Performance Analysis and Channel Optimization", EURASIP J. Inf. Secur., vol. 2014, no. 1, p. 9, 2014.
- [9] T. Langlotz and O. Bimber, "Unsynchronized 4D Barcodes", Proc. 3rd Int. Symp., ISVC 2007, Lake Tahoe, NV, USA, Nov. 26–28, 2007, pp. 363–374.
- [10] C.-Y. Lin and S.-F. Chang, "Distortion Modeling and Invariant Extraction for Digital Image Print-and-Scan Process", Proc. Int. Symp. Multimedia Inf. Process, 1999, pp. 1–10.
- [11] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, "Secret Hiding Mechanism Using FAME-QR Barcode", Proc. IEEE Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS), Dec. 2013, pp. 22–25.
- [12] J. Picard, "Digital Authentication with Copy-Detection Patterns", Proc. SPIE, vol. 5310, pp. 176–183, Jun. 2004.
- [13] M. Querini, A. Grillo, A. Lentini, and G. F. Italiano, "2D color barcodes for mobile phones", Int. J. Comput. Sci. Appl., vol. 8, no. 1, pp. 136–155, 2011.
- [14] M. Querini and G. F. Italiano, "Facial biometrics for 2D barcodes", Proc. IEEE Fed. Conf. Comput. Sci. Inf. Syst. (FedCSIS), Sep. 2012, pp. 755–762.
- [15] J. Rouillard, "Contextual FAME-QR codes", Proc. IEEE 3rd Int. Multi-Conf. Comput. Global Inf. Technol. (ICCGI), Jul/Aug. 2008, pp. 50–55.
- [16] B. Sklar, "Digital Communications", vol. 2. Englewood Cliffs, NJ, USA: Prentice-Hall, 2001.
- [17] Oleskiy J.koval, Thierry pun "Multi Level 2D Bar Codes", Security, Steganography and Watermarking of Multimedia Contents VII, San Jose, California, USA, January 17-20, 2005, Proceedings



**Impact Factor:  
7.512**



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details