ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

Two-Level QR Code For Public - Private Message Sharing and Document Authentication Using Steganography and Machine Learning

Sahil Siddharth Jambhulkar, Vishakha Prashant Ratnaparkhi

Research Scholar, Department of Electronics and Telecommunication, Pune Institute of Computer Technology, Pune, India

Research Scholar, Department of Computer Engineering, Pune Institute of Computer Technology, Pune, India

ABSTRACT: Quick response codes are machine readable optical label which was first created in the automated industry of Japan. Quick response codes are capable enough to store vital information in it by converting into various black and white patterns. Machine learning detects threats by constantly monitoring the behavior of the network for anomalies while generating QR code. Machine learning engines process massive amounts of data in near real time to discover critical incidents. These techniques allow for the detection of insider threats, unknown malware, and policy violations. In this paper researcher used 2 machine learning algorithm to enhance network level security while QR scanning namely Restricted Boltzamine Machine Algorithm and Deep Belief Network Algorithm. QR codes have many applications especially in the field of message sharing and document authentication. The QR code was intended for storage data and fast reading applications. The Quick Response (QR) codes were extensively used in fast reading applications such as statistics storage and high-speed device reading. Anyone can gain get right of entry to data saved in QR codes; hence, they're incompatible for encoding secret statistics without the addition of cryptography or other safety. The novel investigation of this paper represents a visual secret sharing scheme to encode a secret QR code into distinct shares. In assessment with another techniques, the shares in proposed scheme are valid QR codes that may be decoded with some unique that means of a trendy QR code reader, so that escaping increases suspicious attackers. This operation which can effortlessly be achieved the use of smartphones or different QR scanning gadgets. Contribution work is, to maximize the storage size of QR code and generating multi-colored QR code. Experimental outcomes discover that the proposed scheme is feasible and cost is low. Proposed scheme's high sharing performance is likewise recommended in this paper.

KEYWORDS: Division algorithm, error correction capacity, high security, (*k*, *n*) access structure, Quick Response code, visual secret sharing scheme, Machine Learning

I. INTRODUCTION

Using mathematical techniques across huge datasets, machine learning algorithms essentially build models of behaviors and use those models as a basis for making future predictions based on new input data of QR code. Using machine learning to detect malicious activity and stop attacks while generating QR codes. Machine learning algorithms will help businesses to detect malicious activity faster and stop attacks before they get started. The real benefit of machine learning is that it could automate repetitive tasks, enabling staff to focus on more important work. Some believe that machine learning could help close vulnerabilities, particularly zero-day threats and others that target largely unsecured IoT devices.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

In recent years, the QR code is broadly used. In daily life, QR codes are utilizedin an assortment of situations that incorporate information storage, web links, traceability, identification and authentication. First, the QR code is straightforward to be computer equipment identity, for example, mobile phones, scanning weapons. Second, QR code has a large storage capacity, anti-damage strong, reasonably-priced and so on.

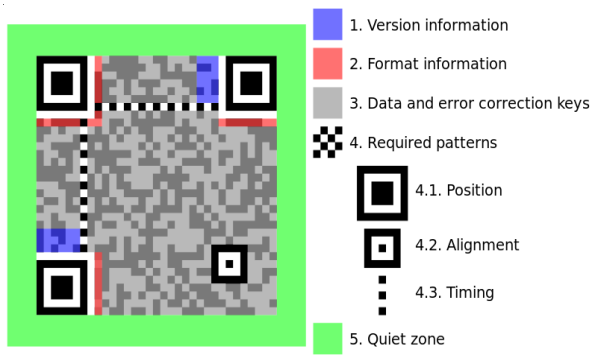

Fig. 1 Specific QR Code Structure

As represented in Fig. 1, the QR code has a unique structure for geometrical correction and high speed decoding. There are three position tags are used for QR code identification and orientation correction. At least one alignment patterns are utilized to code deformation arrangement. The module get it together is set by timing patterns. Furthermore, the format information regions contain error correction level and mask pattern sample. The code version and error correction bits are savedwithin the version information regions.
The popularity of QR codes is primarily due to the accompanying highlights:

1. QR code powerful to the copying procedure,
2. It is effortless to read by utilizing any tool or device and any user,
3. It has excessive encoding capability more desirable with the aid of blunders correction centers,
4. It is in small size and robust to geometrical distortion.

Visual cryptography is another new secret sharing technology. It boosts better the secret share images to restore the complexity of the secret, depending on personal visual decryption. Contrasted and conventional cryptography, it has the benefits of concealment, safety, and the simplicity of secret rebuilding. The method of visual cryptography furnished high safetynecessities of the users and protects them against diverse security attacks. It is simple to generate value in enterprise applications. In this paper, proposed a standard multi-color QR code using textured patterns on data hiding by text steganography and providing security on data by using visual secret sharing scheme.

1.1 Background

The most minimal level can re-establish almost 7% of harmed data, the most elevated amount can re-establish almost 30%. As shown in Fig. 1, the QR code has a particular structure for geometrical adjustment and fast unravelling. Three position labels are utilized for QR code discovery and introduction revision. Three position tags are utilized for QR code discovery and introduction revision. One or more alignment patterns are utilized 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. The QR code era calculation comprises of data encoding utilizing Reed-Solomon blunder redress code, data division on code words, use of veil example, situation of code words and work designs into the QR code. The QR code popularity set of rules consists of the scanning manner, picture, binarization, geometrical correction and interpreting set of rules. The most straightforward sort of rich QR codes is the easy to understand QR code. The focus of these codes is to enhance

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

the tasteful perspective of QR codes. It comprises of changing the hues and state of the modules, or of including a picture into the QR code. Distinctive plan QR 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. As of late, the rich QR code, which includes the essentialness without losing mistake adjustment limit, was presented in [3]. The creators proposed a novel technique for mixing a shading picture into the QR code, which adjusts the QR code source pixels so that the white (rsp. dark) module pixels are changed from white (rsp. dark) to any RGB values and whose luminance esteem is considered as white (rsp. dark) pixel by QR code binarization technique. Recently, the QR code steganography, which aims to hide a secret message into a QR code, was introduced.

1.2 Motivation

The motivation of the work is to propose the storage capacity limit can be essentially enhanced by expanding the code letters in order qor by expanding the textured pattern size. It expands the storage capacity limit of the established QR code. It provides security for private message using visual secret sharing scheme. QR code was created by Denso Wave in Japan while working for car industry in 1994.QR codes are basically a two- dimensional bar codes which are used day by day due to the technological advancements. These codes have a lot of uses. To give some examples, these QR codes can be utilized for putting away data, site diverting, following and following (for transportation tickets or brands), Entity distinguishing proof (traveler data, general store items), Uniform asset locator, Code instalments, Virtual stores, Website login, Message sharing and record verification. Subsequently of which the interest for QR code scanners has additionally expanded relatively. The prevalence of QR code is due to its robustness, easy to read feature, higher encoding capacity and small size. The accreditation of QR code was performed by Worldwide Organization of Standardization (ISO), and its entire particular can be found in [1]. A QR code encodes the data into binary form. Every data bit is represented by a black or a white module. The Reed-Solomon error correction code [2] is utilized for data encryption. Therefore, one of 4 error correction levels have picked during QR code generation.

1.3 Objectives of the paper

1. To hide secret information in QR image.
2. To develop a private message sharing mechanism which is the invisible storage and transmission of private information into QR code.
3. To print document authentication, to verify whether the printed document is an original or a copy.
4. To increase the storage capacity.
5. To distinguish the original printed document from its copy.

1.4 Problem Statement

Proposed system formulate problem for replacement of modules by adding pixel from cover image. Additionally while using QR code for data security information is encoded by text steganography. QR code image is encrypted with patches extracted from cover image for security by texture synthetic image analysis. Proposed work also design problem for adding noise to QR code data.

1.5 Goals of the paper

1. Improve pattern recognition by supervised learning QR code image.
2. Image Steganography for patch processing.
3. Cover the textured pattern analysis to automate its combination process for QR code.
4. Recover message from QR code by cropping and reconstructing.
5. Replacing white modules with additional pixel.
6. Apply cover image over generated QR code.
7. Using QR code for social network service.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

II. REVIEW OF LITERATURE

The paper [1] proves that the contrast of XVCS is $2^{(k-1)}$ times greater than OVCS. The monotone property of OR operation reduces the visual quality of reassembled image for OR-based VCS (OVCS). Accordingly, XOR-based VCS (XVCS), which makes use of XOR operation for decoding, turned into proposed to enhance the contrast. Advantages are: Easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS. Disadvantages are: Proposed algorithm is more complicated.

In [2] paper, present a visually impaired, key based watermarking technique, which embeds a transformed binary form of the watermark data into the DWT domain of the cover image and uses an extraordinary image code for the identification of image distortion. The QR code is inserted into the attack resistant HH part of 1stlevel DWT area of the cover image and to distinguish malicious interference by an attacker. Advantages are: More information representation per bit change combined with error correction capabilities. Increases the usability of the watermark data and maintains robustness against visually invariant data removal attacks. Disadvantages are: Limited to a LSB bit in the spatial domain of the image intensity values. Since the spatial space is progressively defenseless to attcks this can't be utilized.
In [3] paper, design a secret QR sharing way to deal with ensure the private QR information with a safe and reliable appropriated framework. The proposed methodologyvaries from related QR code schemes in that it utilizes the QR qualities to accomplish secret sharing and can oppose the print-and-scan activity. Advantages are: Reduces the security risk of the secret. Approach is feasible. It provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. Disadvantages are: Need to improve the security of the QR barcode. QR technique requires reducing the modifications.

The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication [4]. The public level is the same as the same standard QR code storage level; therefore it is readable through any classical QR code utility. The private level is built by using changing the black modules throughprecise textured patterns. It comprises of information encoded using q_ary code together an error correction capability. Advantages are: It increases the storage capacity of the classical QR code. The textured patterns used in 2LQR sensitivity to the P&S process. Disadvantages are: Need to improve the pattern recognition method. Need to increase the storage capacity of 2LQR by replacing the white modules with textured patterns.

To secure the sensitive data, [5] paper investigates the qualities of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload contrasted with the previous ones. For anordinary scanner, a browser can just screen the formal information from the stamped QR code. Advantages are: The designed scheme is feasible to hide the secrets into a modest tiny QR tag as the motivation of steganography. Only the authorized user with the private key can correspondingly screen the secured secret successfully. Disadvantages are: Need to increase the security.

The paper [6] refers the authentication problem of real-world goods on which 2D bar-codes (2D-BC) were printed and take the challengers view. The challengers are assumed to have access to noisy copies of an original 2D-BC. A simple estimator of the 2D-BC is depends on copies averages is proposed, letting the challengers print a fake 2DBC with as original by the system detector. Performance of the estimator in terms of error probability on the detector side is then derived with admire to Nc and compared with experimental outcomes on actual 2D-BC. It is shown that the adversary can produce a fake that successfully fools the detector with a reasonable number of genuine goods. Advantage: Create a fake 2D-BCs declared as genuine by the detector. Disadvantage: Require additional noise to generate fake barcode. Generating fake 2D QR code declared as original by QR code reader.

The paper [7] proposes strategy for concealing secret information dependent on bit system is so fragile to adjustment attack. Storing secret data dependent on bit technique is so yield to update attack. If an attacker exchange any bit of hidden bits, it is far difficult to recover the secret data. So from this paper, refer a scheme dependent on Reed- Solomon codes and List Decoding to conquer this issue. Likewise direct our solution by dissecting the complexity, security, and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

analysis. Advantage: For attacker hard to discover original data Reed-Solomon codes and List Decoding to overcome this issue. In this paper, refer Reed-Solomon codes for encoding content in QR code.

The paper [8] represents no direct connection between devices can exist. Time-multiplexed, 2D colors barcodes are show on screen & recorded with camera embed mobile phones. A Proposed techniqueoffers optical information transfer between public presentations and mobile devices primarily based on unsynchronized 4D barcodes. After, recall that no direct connection among the devices can exist. Time-multiplexed, 2D color barcodes are displayed on screens and recorded with camera prepared mobile phones. This permits transmitting information optically between both devices. Advantage: Maximizes the data throughput and the robustness of the barcode recognition. In this paper, refer Time-multiplexed, 2D color barcodes.

The paper [9] indicates properties of the undermined, rescanned image in both the spatial and frequency areas, and after that further examines the adjustments in the Discrete Fourier Transform (DFT) coefficients. In view of these properties, demonstrate several methods in paper for separating invariants from the original and rescanned image, with potential applications in image watermarking and authentication. Advantage: Authentication by image watermarking. Disadvantage: Uses watermarking based authentication. In this paper, Discrete Fourier Transform coefficients and image based authentication is utilized.

The paper [10] describes the proposed plan can disguise the secret data into the cover QR code without distorting the intelligibility of QR content. That is, widespread browsers can read the QR content from the marked QR code for the sake of reducing interest. Only the legal receiver can encrypt and retrieve the secret from the marked QR code. The secret payload of the designed scheme is alterable. The scheme can bring larger secret into a QR code as reported by the selection of the QR version and the error correction level. Advantage: Only the authorized receiver can encrypt and retrieve the secret from the marked QR code. Secret hiding mechanism used for QR code by encrypted payload.

III. OPEN ISSUES

A QR code is robust to segmental loss or symbol damage. Any user can access the information in QR codes; therefore, they are unsuitable for storing secret data. During the past few years, many efforts have been made to place and protect secret messages in QR codes. Existing system based on searching relational values between P&S un-useful patterns and related patterns. The storage capacity can be magnificently increased by code alphabet q or by increasing the textured pattern size. Existing system results show a restoration of private information. It also highlights the possibility of using this QR code for document authentication.

Advantages are:-

Increase storage capacity of QR code along with differentiate original document.

Disadvantages are:-

1. QR codes are unsuitable for storing secret data.
2. The computational overhead of all the aforementioned schemes is slightly larger.
3. Data stored in a QR code is can be easily readable to camera containing, although it is not plain text and therefore is only readable to authorized user, likewise watch and read.
4. It is impossible to classify an originally document in QR code from its copy due to their insensitivity to the Print and Scan process.

IV. PROPOSED METHODOLOGY

In this paper, an innovative scheme is proposed to improve the security of QR codes using the XVCS theory. First, an improved (n, n) sharing method is designed to avoid the security weakness of existing methods. On this basis, consider the method for (k, n) access structures by utilizing the (k, k) sharing instance on every k-participant subset, respectively. This approach will require a large number of instances as n increases. Therefore, presents two division

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

algorithms to classify all the k-participant subsets into several collections, in which instances of multiple subsets can be replaced by only one.

1. Enhanced (n, n) sharing method
2. (k, n) sharing method

Based on the enhanced (n, n) method, a (k, n) method can be achieved if apply the (k, k) instance to every k-participant subset of the (k, n) access structure. However, there will be a huge amount of (k, k) instances.

I. Architecture

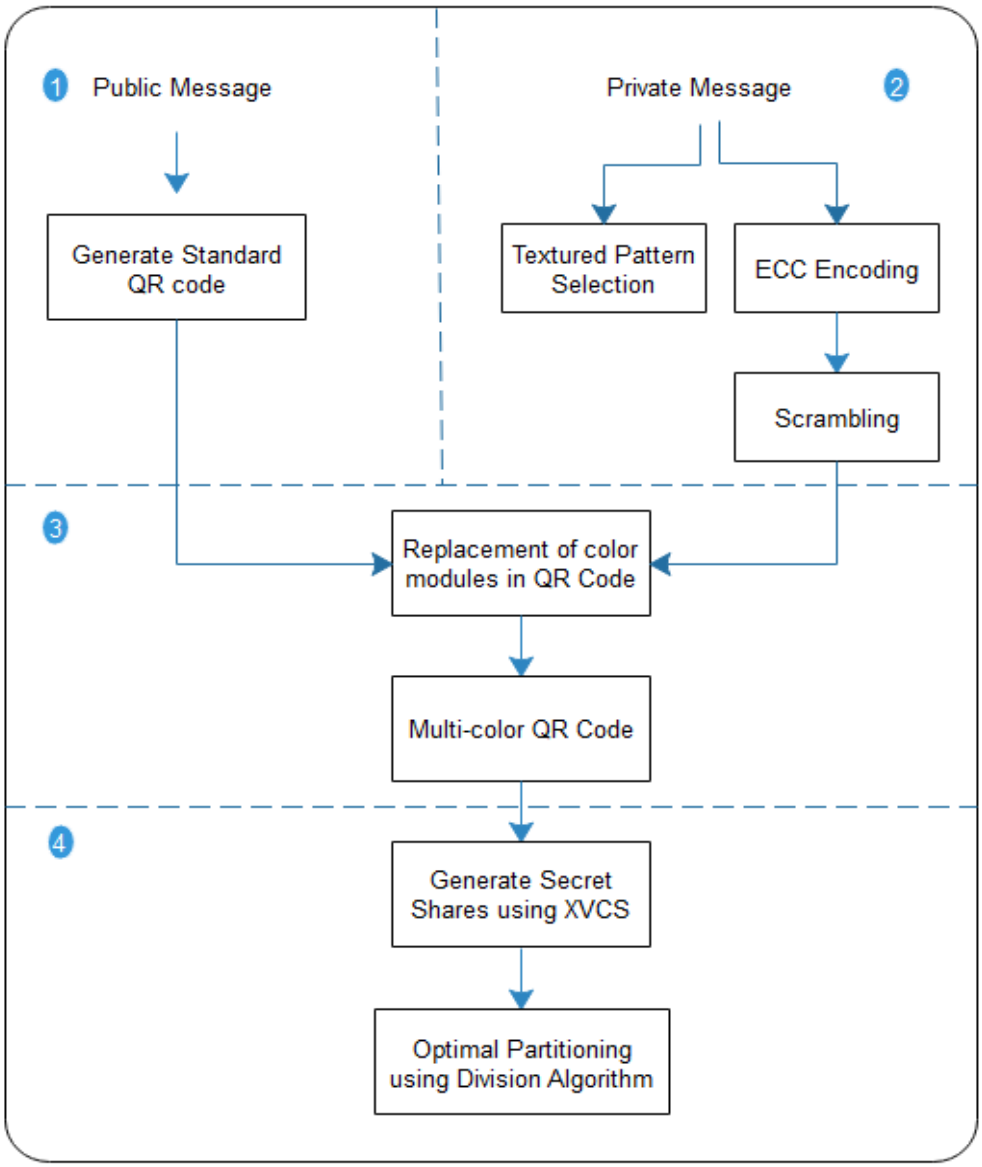

Fig. 2 Proposed System Architecture

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

Advantages are:

1. Secure encoding of document or text.
2. Text steganography for message encoding.
3. Increases the sharing efficiency.
4. VCS is low computational complexity.
5. Higher security and more flexible access structures.
6. Computation cost is less.
7. stego synthetic texture for QR code hiding.

II. Mathematical Model

Two collections of $n \times 1$ Boolean matrices denoted by C^0 and C^1 consist of an (n, n)-XVCS if the following conditions are satisfied:

1) $If\ X = P, then\ \forall B \in C^0(C^1), w(B_P) = 0(1).$

2) $If\ X \subseteq P\ and\ X \subseteq P, then\ \forall B \in C^0\ or\ C^1;\ the\ possibilities\ of\ w(B_X) = 0\ and\ w(B_X) = 1\ are\ equal.$ (2)

The first property is contrast, which illustrates that the secret can be recovered by XOR-ing all participant shares. The second property is security, which prevents any k (k <n) participants from gaining any knowledge of the secret.

Enhanced (n, n) sharing method

Define two blocks B_1 and B_2 belong to an identical group G if $B_1 = B_2$ is satisfied. (3)

With above definition, can divide $T_1^q, T_2^q, \dots, T_n^q$ into several groups $G_1^q, G_2^q, \dots, G_u^q$. For example, to determine whether T_1^q and T_2^q are of a same group, calculate $T_1^q \oplus T_2^q$. If $T_1^q \oplus T_2^q = 0$, then can conclude that T_1^q and T_2^q are of an identical group, and vice versa. A block different from any other blocks will not be contained in any group.

$T^q(i)$ is said to be responsible for $S^q(i)$ if $T^q(i,j)$ is reversed to share $S^q(i,j)$.

Let $X_{ki} = 1$ denote the case that $T_k^q(i)$ is responsible for $S^q(i)$ and let $X_{ki} = 0$ represent the opposite. A matrix X is constructed by solving (1).

$$X = \begin{bmatrix} \overbrace{x_{11}\ x_{12} \cdots x_{1d}\ 00\cdots0}^{c} \\ x_{21}\ x_{22} \cdots x_{2d}\ 00\cdots0 \\ \vdots\ \vdots\ \ddots\ \vdots\ \vdots\ \ddots\ \vdots \\ \underbrace{x_{n1}\ x_{n2} \cdots x_{nd}}_{d}\ \underbrace{00\cdots0}_{c-d} \end{bmatrix}$$

$$\begin{cases} \sum_{q=1}^{n} X_{pq} \le r (p = 1,2,\dots,n) \\ \sum_{q=1}^{d} (X_{iq} | X_{jq}) \ge d - c + r + 1 (T_i^q \ne T_j^q \in G_k^q; k = 1,2,\dots,u) \\ \sum_{q=1}^{d} (X_{1q} | X_{2q} | \dots | X_{nq}) = d \\ X_{pq} \in \{0,1\} (q = 1,2,\dots,d; p = 1,2,\dots,n) \end{cases} \quad (4)$$

If n satisfies the condition $n \times r \ge c - r$, there must be a solution to (1) when $d = c - r$. In addition, adjust the value of d ($c - r \le d \le c$) to balance errors between the covers and the reconstructed secret. Based on X, design a new sharing algorithm.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

III. Algorithms

1. Creating a QR Code

Encoding:-

Representation of each letter in secret message by its comparable ASCII code.

1. Conversion of ASCII code to comparable 8 bit binary number.
2. Division of 8 bit binary number into two 4 bit parts. Selecting of suitable letters comparing to the 4 bit parts.
3. Meaningful sentence development by utilizing letters got as the primary letters of appropriate words.
4. Omission of articles, pronoun, relational word, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding procedure to give adaptability in sentence development.
5. Encoding isn't case sensitive.

Decoding:-

Steps:

1. First letter in each expression of cover message is taken and represented by corresponding 4 bit number.
2. 4 bit binary numbers of joined to get 8 bit number.
3. ASCII codes are gotten from 8 bit numbers.
4. Finally secret message is recovered from ASCII codes.

2. Sharing Algorithm

Input: $C_1, C_2, \dots, C_n$ and S (Each QR code has a blocks).

Output: $T_1, T_2, \dots, T_n$.

Step 1: Let $i \longleftarrow 1,\ q \longleftarrow 1\ and\ T_k \longleftarrow C_k\ (1 \le k \le n)$. Go to Step 2.

Step 2: According to (2), groups $G_1^q, G_2^q, \dots, G_u^q$ are determined by pairwise XOR-ing $T_1^q, T_2^q, \dots, T_n^q$ (u may be different when q changes). Go to Step 3.

Step 3: Based on $G_1^q, G_2^q, \dots, G_u^q$, obtain the solution to (1). Then, X is also obtained, go to Step 4.

Step 4: Conduct a row permutation on the rows according to the elements of $G_k^q (1 \le k \le u)$, respectively. In addition, permute those rows which are not included in any group and go to Step 5.

Step 5: Perform a column permutation on all columns of X and go to Step 6.

Step 6: Count the number of 1 in column i of X and denote it as t_i. If $t_i > 1$, let $k \longleftarrow 1$ and go to Step 7; else if $t_i = 1$, go to Step 9; else go to Step 10.

Step 7: If $X_{ki} = 1$, then for each $j\ (1 \le j \le 8)$, we randomly assign 0 or 1 to $T_n^q(i,j)$ and let $X_{ki} = 0$; else, skip. Go to Step 8.

Step 8: Let $t_i \longleftarrow t_i \longleftarrow 1$. If $t_i > 1$, let $k \longleftarrow k + 1$ and go to Step 7; else, go to Step 9.

Step 9: Find the p that has $x_{pi} \longleftarrow 1$. Then, for each $j\ (1 \le j \le 8)$, calculate $t \longleftarrow T_1^q(i,j) \oplus T_2^q(i,j) \oplus \dots \oplus T_n^q(i,j)$. If $t \longleftarrow S^q(i,j), T_p^q(i,j) \longleftarrow \sim T_p^q(i,j)$; else, skip. Go to Step 10.

Step 10: Let $i \longleftarrow i + 1$. If $i \le c$, go to Step 6; else, let $i \longleftarrow 1$ and go to Step 11.

Step 11: Let $q \longleftarrow q + 1$. If $q \le a$, go to Step 2; else, go to Step 12.

Step 12: Algorithm ends.

3. Division Algorithm 1

Input: A collection of all k-participant subsets M_0.

Output: Divided collections $M_1, M_2, \dots, M_d$. (dis the number of collections)

Step 1: Let $i \longleftarrow 1, P \longleftarrow \{1, 2, \dots, n\}, P_1 \longleftarrow \emptyset, P_2 \longleftarrow \emptyset, \dots, P_k \longleftarrow \emptyset, g \longleftarrow 0, r \longleftarrow 0$, and $d \longleftarrow 0$, go to Step 2.

Step 2: Randomly select a subset Q from M_0 and suppose $Q = \{i_1, i_2, \dots, i_k\}$. Let $P' \longleftarrow P - Q = \{i_{k+1}, i_{k+2}, \dots, i_n\}$. If $|P'| = n - k \le k$, go to Step 3; else, let $g \longleftarrow \lfloor n / k \rfloor$ and $r \longleftarrow n - g.k$ and go to Step 4.

Step 3: Let $P_1 \longleftarrow \{i_1, i_{k+1}\}, P_2 \longleftarrow \{i_2, i_{k+2}\}, \dots, P_{n-k} \longleftarrow \{i_{n-k}, i_n\}, P_{n-k+1} \longleftarrow \{i_{n-k+1}\}, \dots, P_k \longleftarrow \{i_k\}$ and go to Step 5.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

Step 4: Let $P_1 \longleftarrow \{i_1, i_{k+1}, \dots, i_{gk+1}\}, P_2 \longleftarrow \{i_2, i_{k+2}, \dots, i_{gk+2}\}, \dots, P_r \longleftarrow \{i_r, i_{k+r}, \dots, i_{gk+r}\}, P_{r+1} \longleftarrow \{i_{r+1}, i_{k-r+1}, \dots, i_{(g-1)k+r+1}\}, \dots, P_k \longleftarrow \{i_k, i_{2k}, \dots, i_{gk}\}$ and go to Step 5.
Step 5: Choose $i_{p_1} \in P_1, i_{p_2} \in P_2, \dots, i_{p_k} \in P_k$to constitute a subset $\{i_{p_1}, i_{p_2}, \dots, i_{p_k}\}$. Then, let all such possible subsets consist of the collection $M_i$and go to Step 6.
Step 6: Let $M_0 \longleftarrow M_0 - M_i, d \longleftarrow i, i \longleftarrow i + 1$. If $M_0 \neq \emptyset$, redefine all participants of M_0 as P and let $n \longleftarrow |P|$ and go to Step 2; else, go to Step 7.

4. Division Algorithm 2
Input: A collection of all k-participant subsets M_0.
Output: Divided collections $M_1, M_2, \dots, M_d$. (dis the number of collections)
Step 1: Let $i \longleftarrow 1, d \longleftarrow 0$ and go to Step 2.
Step 2: Randomly select a subset Q from M_0 and suppose $Q = \{i_1, i_2, \dots, i_k\}$. Let $Q \in M_i$, and go to Step 3.
Step 3: Search the remaining subsets in M_0. If the model above remains solvable when we assume that $Q' \in M_i$, then let $Q' \in M_i$. Go to Step 4.
Step 4: Let $M_0 \longleftarrow M_0 - M_i, d \longleftarrow i, i \longleftarrow i + 1$. If $M_0 \neq \emptyset$, go to Step 2; else, go to Step 5.
Step 5: Algorithm ends.

5. Restricted Boltzamine Machine Algorithm
$x_1$is a sample from the training distribution for the RBM
ϵ is a learning rate for the stochastic gradient descent in Contrastive Divergence
$W$is the RBM weight matrix, of dimension (number of hidden units, numbr of inputs)
$b$is the RBM offset vector for input units
$c$is the RBM offset vector for hidden units
Notation: $Q(h_{2_i} = 1|x_2)$is the vector with elements $Q(h_{2_i} = 1|x_2)$
Step 1: for all hidden units i do
Step 2: compute $Q(h_{1_i} = 1|x_1)$(for binomial units, $sigm(c_i + \sum_j W_{ij}\, x_{1j})$)
Step 3: sample $h_{1_i} \in \{0,1\}$from $Q(h_{1_i}|x_1)$
Step 4: end for
Step 5: for all visible units j do
Step 6: compute $P\left(x_{2_j} = 1\middle|h_1\right)$(for binomial units, $sigm(b_j + \sum_i W_{ij}\, h_{1i})$)
Step 7: sample$x_{2_j} \in \{0,1\}$from $P\left(x_{2_j} = 1\middle|h_1\right)$
Step 8: end for
Step 9: for all hidden units j do
Step 10: compute $Q(h_{2_i} = 1|x_2)$(for binomial units, $sigm(c_i + \sum_j W_{ij}\, x_{2j})$)
Step 11: end for
Step12: $W \longleftarrow W + \epsilon(h_1 x_1' - Q(h_{2_i} = 1|x_2)x_2')$
Step 13: $b \longleftarrow b + \epsilon(x_1 - x_2)$
Step 14: $c \longleftarrow c + \epsilon(h_1 - Q(h_{2_i} = 1|x_2))$

6. Deep Belief Network Algorithm
Train a DBN in a purely unsupervised way, with the greedy layer-wise procedure in which each added layer is trained as an RBM (e.g., by Contrastive Divergence).
$\hat{P}$is the input training distribution for the network
ϵ is a learning rate for the RBM training
ℓ is the number of layers to train

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

$W^k$is the weight matrix for level k, for k from 1 to ℓ
$b^k$is the visible units offset vector for RBM at level k, for k from 1 to ℓ
$c^k$is the hidden units offset vector for RBM at level k, for k from 1 to ℓ
Mean_field_computation is a Boolean that is true iff training data at each additional level is obtained by a mean-field approximation instead of stochastic sampling
Step 1: for k = 1 to ℓdo
Step 2: initialize $W^k = 0, b^k = 0, c^k = 0$
Step 3: while not stopping criterion do
Step 4: sample $h^0 = x$ from $\hat{P}$
Step 5: for $i = 1$ to $k - 1$do
Step 6: if mean_field_computation then
Step 7: assign h_j^i to $Q(h_j^i = 1|h^{i-1}$, for all elements j of h^i
Step 8: else
Step 9: assign h_j^i to $Q(h_j^i|h^{i-1}$, for all elements j of h^i
Step 10: end if
Step 11: end for
Step 12: RBMupdate($h^{k-1}, \in, W^k, b^k, c^k$) {thus providing $Q(h^k|h^{k-1})$for future use}
Step 13: end while
Step 14: end for

V. RESULT AND DISCUSSIONS

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcat server. Some functions used in the algorithm are provided by list of jars like zxing jar for QR code generation etc.The multi-color QR code security with texture patterns by applying the X-ORing based Visual Cryptography Scheme on QR code for sharing secrets to the receiver. The fig. 3 shows the multi-color QR code example. The experiment includes two processes encryption process and decryption process.

Input:

Fees: Admission Fees
Total: 5700.0
Name: ShilpaTandale
Bank Name: Kotak Bank-
5678123323454567-
05/2022-732

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

Output:

Fig. 3 Multi-color QR code

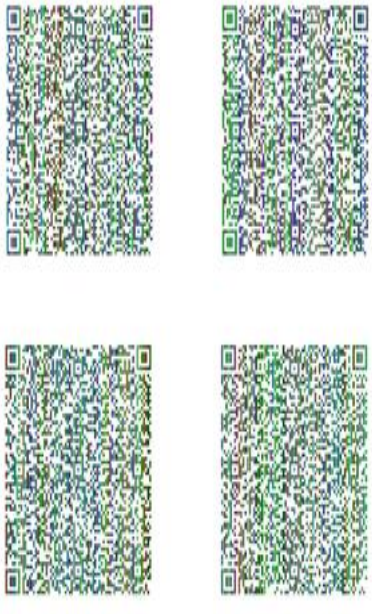

Fig. 4 XVCS using Secret Shares generated of given message (n=4, k=3)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

gc:wy1r3z-r//gc0bx2-jfg40f-vz3qqf-ema65m-96y2fh-z8jmg5-rvan1g-y16tar-dzj06b-5a1q71-3n5vep-ak00an-74z2td-9zt59p-jzv3dx-rap5k0-vnt8cv-s5kcsh-tayqgc-cc7y42-6zzn4m-8pxhnw-x2nc8b-x3chr8-6ykpbs-agd1dy-82ssw4-0xq7x1-vkfm8c-4wbkrm-daeca0-yy6tfd-3h66cs-eh7zgq-10kryc-4pqg8r-nqvqyb-5pw72g-8npcmz-yakj6v-eemga6-0yxqdz-7z7e3k-kbbagh-0nd17s-a353vf-60bvtc-m97fh6-69zwx2-0h9x3n-dhdk56-317r70-dfkn4y-vtefax-qazw1r-x065n5-w2be8

gc:wy1r3z-r//g9mh8k-m1a3zr-4jm0n8-4dy85h-7eax3b-kr5v8t-bcmhdr-hcret0-gzq7ht-rdwzhp-5t5mth-gyh1c6-cw827v-30dywt-gmfd6n-sms02f-vjs9bv-az2cmd-ybxqf9-kxwncg-b5pbzj-qar3p6-cqc43e-jpzsra-9arwj3-qa5ysc-q1hsya-fdbadk-j6jnng-vsv5aa-fme8h5-1vqbh5-fpp338-ft0x7v-kwf1qd-a0mxqp-stqcys-r42xfe-trp5q2-rv9g2v-j52wgg-c3vq4p-gzbmfa-bnhpwx-jscw4a-f6885y-vzwp3j-b2r5gx-deevq6-4a3mp8-j7c8fs-gfw4ns-jtj56x-34vwks-3tmntx-k9mwxx-w4

gc:wy1r3z-r//g9e68k-w103th-a1mc9x-rdxhnn-vd6j3w-1nfpwp-5gd8ex-s4rnn1-9gd4da-tarc50-xqm12d-nst5xd-x04y6n-nr87y7-h7c3e4-b26gtt-cf7wj4-hbrdxa-xmc1be-7tc44b-hvjtc2-ysvea2-n6xct2-mmsjcj-hkegmw-dx1t93-ks98c3-e30xg4-jhjjqg-zgbex6-cm14r8-9xymf9-z6grnd-tbxqb0-vgj0vp-hq2eg4-pxetea-r6ha4q-vcywc9-9ywk8g-xmskga-x9z05k-h2y6g0-jya2aw-m8k0k7-7k2a2t-jnwykc-6vw0qv-sejfkw-7sjg27-mxp9zv-z6q4c2-9p0bnz-scn5wj-511eb6-yyzkj5-7ym0

Fig. 5 shows the secret shares generated of given message, it has given contents given below.

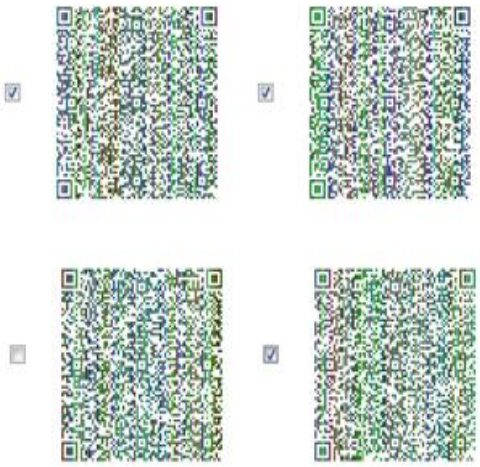

Fig. 6 Retrieve the original message

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

At Receiver selects the 3 secret parts for reconstructing the original message.

Output:

Fees: Admission Fees
Total: 5700.0
Name: ShilpaTandale
Bank Name: Kotak Bank-
5678123323454567-05/2022-732

Fig. 6 shows an explicit comparison of the number of (k, k) instances. The changes are significant regardless of whether Division Algorithm 1 or Division Algorithm 2 is implemented. Additionally, in most (k, n) values, the number of (k, k) instances is reduced when Division Algorithm 1 is used rather than Division Algorithm 2. Thus, using Division Algorithm 1 results in a smaller number of shares and a greater sharing efficiency. However, Division Algorithm 2 is more suitable than Division Algorithm 1 for scenarios in which the shares are all different from each other.

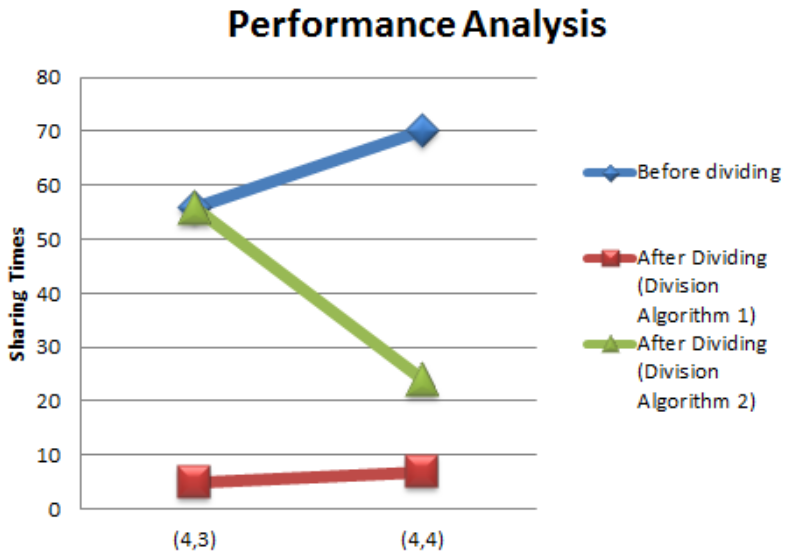

Fig. 7 Performance analysis of the number of (k, k)-XVCS instances

Table I Performance on reduction of sharing instances

(n, k)	Before dividing	After Dividing 1	Decreasing ratios 1	After Dividing 2	Decreasing ratios 2
(4,3)	56	5	91.07	56	0
(4,4)	70	7	90	24	65.71

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

VI. CONCLUSION

In this paper, proposed a visual secret sharing scheme for QR code applications, which makes improvement mainly on two aspects: higher security and more flexible access structures. In addition, extended the access structure from (*n*, *n*) to (*k*, *n*) by further investigating the error correction mechanism of QR codes. In this paper researcher used 2 machine learning algorithm to enhance network level security while QR scanning namely Restricted Boltzamine Machine Algorithm and Deep Belief Network Algorithm. QR codes have many applications especially in the field of message sharing and document authentication Two division approaches are provided, effectively improving the sharing efficiency of (*k*, *n*) method. Therefore, the computational cost of our work is much smaller than that of the previous studies which can also achieve (*k*, *n*) sharing method. The future work will make the QR code reader for scanned QR code within fraction of seconds.

REFERENCES

[1] Y. Cheng, Z. Fu and B. Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2393-2403, Sept. 2018.
[2] C. N. Yang, D. S. Wang, "Property Analysis of XOR-Based Visual Cryptography," IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.
[3] P. P. Thulasidharan, M. S. Nair, "QR code based blind digital image watermarking with attack detection code," *AEU - International Journal of Electronics and Communications*, vol. 69, no. 7, pp. 1074-1084, 2015.
[4] P. Y. Lin, "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 384-392, 2016.
[5] I. Tkachenko, W. Puech, C. Destruel, *et al.*, "Two-Level QR Code for Private Message Sharing and Document Authentication," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 13, pp. 571-583, 2016.
[6] P. Y. Lin, Y. H. Chen, "High payload secret hiding technology for QR codes," *Eurasip Journal on Image & Video Processing*, vol. 2017, no. 1, pp. 14, 2017.
[7] C. Baras and F. Cayre, "2D bar-codes for authentication: A security approach," in Proc. 20th Eur. Signal Process. Conf. (EUSIPCO), Aug. 2012, pp. 1760–1766.
[8] T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, "Robust message hiding for QR code," in Proc. IEEE 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP), Aug. 2014, pp. 520–523.
[9] T. Langlotz and O. Bimber, "Unsynchronized 4D barcodes," in 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," in 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 QR barcode," in Proc. IEEE Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS), Dec. 2013, pp. 22–25.
[12] Nathan shone , trannguyenngoc, vu dinhphai , and qi sh, "a deep learning approach to network intrusion detection", ieee transactions on emerging topics in computational intelligence, vol. 2, no. 1, february 2018
[13] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in Proc. 8th IEEE Int.Conf. Commun. Softw. Netw, Beijing, China, Jun. 2016, pp. 581–585.
[14] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in Proc. 15th IEEE Int. Conf. Mach. Learn. Appl., Anaheim, CA, USA, Dec. 2016, pp. 195–200.
[15] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proc. 9th EAI Int.Conf. Bio-Inspired Inf. Commun. Technol., 2016, pp. 21–26. [Online].
[16] S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced intrusion detection system," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom.*, Berlin, Germany, Sep. 2016, pp. 1–8.
[17] C. Garcia Cordero, S. Hauke, M. Muhlhauser, and M. Fischer, "Analyzing flow-based anomaly intrusion detection using replicator neural networks," in *Proc. 14th Annu. Conf. Privacy, Security. Trust*, Auckland, New Zeland, Dec. 2016, pp. 317–324.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

[18] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *Proc. Int. Conf. Wireless Netw. Mobile Commun.*, Oct. 2016, pp. 258–263.

[19] C. Yin, Y. Zhu, J. Fei and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," in *IEEE Access*, vol. 5, pp. 21954-21961, 2017.

[20] Revathi, S &Malathi, A. (2013). A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection. International Journal of Engineering Research & Technology (IJERT). 2. 1848-1853.

[21] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," in *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41-50, Feb. 2018.

[22] Anomaly-based network intrusion detection: Techniques, systems and challenges Garcia-Teodoro P. Diaz-Verdejo J., Macia-Fernandez G., Vazquez E. (2009) *Computers and Security*, 28 (1-2), pp. 18-28.

[23] Claude Turner*, Rolston Jeremiah, Dwight Richards, Anthony Joseph, "A Rule Status Monitoring Algorithm for Rule-Based Intrusion Detection and Prevention Systems", Procedia Computer Science, ISSN: 1877-0509, Vol: 95, Page: 361-368, 2016

[24] R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, "Deep learning and its applications to machine health monitoring: A survey," Submitted to IEEE Trans. Neural Netw. Learn. Syst., 2016. [Online]. Available: http://arxiv.org/abs/1612.07640

[25] H. Lee, Y. Kim, and C. O. Kim, "A deep learning model for robust wafer fault monitoring with sensor measurement noise," IEEE Trans. Semicond. Manuf., vol. 30, no. 1, pp. 23–31, Feb. 2017.

[26] L. You, Y. Li, Y. Wang, J. Zhang, and Y. Yang, "A deep learning based RNNs model for automatic security audit of short messages," in Proc. 16th Int. Symp. Commun. Inf. Technol., Qingdao, China, Sep. 2016, pp. 225–229.