Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN : 2348-4470
p-ISSN : 2348-6406

International Journal of Advance Engineering and Research Development

Special Issue on Recent Trends in Data Engineering

Volume 4, Special Issue 5, Dec.-2017

Survey Paper on Document Authentication using Color QR Codes

Prof. S. N. Zaware[1], Aswathy Sreenivasan[2], Pratik Kulkarni[3], Rasika Pawar[4], Shraddha Chavan[5]

[1]*Department of Computer Engineering, AISSMS Institute of Information technology,Pune,Maharashta,India*
[2]*Department of Computer Engineering, AISSMS Institute of Information technology,Pune,Maharashta,India*
[3]*Department of Computer Engineering, AISSMS Institute of Information technology,Pune,Maharashta,India*
[4]*Department of Computer Engineering, AISSMS Institute of Information technology,Pune,Maharashta,India*
[5]*Department of Computer Engineering, AISSMS Institute of Information technology,Pune,Maharashta,India*

ABSTRACT: *Quick Response (QR) codes are now extremely popular due to the widespread uses of smart phones. Almost all the areas have had the QR codes to overtake the traditional one-dimensional bar codes, due to the increased capacity and quick data retrieval. QR codes offer a myriad of specifications like small space, durability against damage due to soil, better data capacity and higher language support, which make them much better than bar codes. Further, this Project is attempting expand the size of the QR codes further by making use of Color QR codes, which are generated using the process of multiplexing black and white QR codes. Extremely quick results can be achieved by multiplexing and de-multiplexing of QR codes when less than 12 are used. Blowfish algorithm is efficient. This has been proved due by measuring the time required for its execution as well as its throughput. Due to the use of large key size, the efficiency of the algorithm may be affected. Further, the data which is considered is encrypted using Blowfish Algorithm, which makes the data secure and tamper-proof. Blowfish Algorithm belongs to the class of the algorithms which have a symmetric block cipher. The block cipher has a size of 64 bits and the key is variable, having a key length which can range from 32 bits until 448 bits at the maximum. This algorithm is a very fast and a useful scheme. It consists of a sub-key, an S-box phase and the actual encryption phase.*

Keywords: *QR codes, Color QR codes, multiplexing, de-multiplexing, Blowfish Algorithm*

I. INTRODUCTION

The results which are displayed online by Savitribai Phule Pune University are accessible to anyone who knows the seat number of a particular student. This access can enable any person to manipulate the result without the knowledge of the student. Furthermore, the student can himself manipulate his own result. This may give that particular student an unfair advantage.

To avoid such malpractices, there must be a way of providing security to these digital results, which in turn provide security to the actual hard copy of the result. To provide a way to individualize these extremely important and sensitive digital results, as well as to avoid tampering them and thereby avoiding any kind of malpractice, this Project has been considered.

The Project makes use of two-dimensional Color QR codes for encrypting the digital copy of the result. This encryption of the result allows the result to be seen only by the respective student or by a legitimate registered party besides the University itself or the College authorities of that student.

To access the digital result, a quick as well as a secure way has to be provided, unlike the customary method which requires only the seat number. Quick Response codes are a utilitarian option for this. The QR codes are extremely common nowadays and can be accessed by any person with a basic smart phone.

Further to encrypt the student's mark sheet, the Blowfish Algorithm has been used. Using this encryption algorithm, the mark sheet can be accessed only by the particular student. If there are any changes in the mark sheet, they can be detected due to the fact that the encryption key, which has been generated using the Blowfish Algorithm, changes even if there is a change in a single bit in the original document. This in turn changes the QR codes which have been generated, and makes the QR code invalid.

The current University results which are displayed online have no method of encryption or any kind of hashing algorithm to prevent the manipulation of the result. The result can be accessed by entering the seat number of a particular student along with his/her mother's name. Both the fields can easily be acquired by any person, without much effort and research.

This method can and has been extremely inefficient when it comes to protecting the results' privacy. A QR code is accompanied by the result, which instead of being unique for a particular student, redirects to the website of the University, which displays the result by entering the above mentioned credentials. There is no actual method to verify if the document, which is the result in this case, is authentic apart from actually confirming it with the University or the academic Institution, which the student has passed from, both of which require a significant amount of effort due to which it is usually neglected.

Cryptography is the technology which is extensively used in the field of network security. As a core concept, the data should be confidential and authentic. The message which has to be sent, viz. the plain-text, and the encrypted or encoded message which is called the cipher text are used in cryptography. The process of transforming the plain-text to the encrypted cipher text is known as the encrypting process. The reverse process is known as the decryption process. .

Cryptographic algorithm is classified as:

1. Symmetric Key Cryptography, in which a single key is used in case of encryption and decryption. .
2. Asymmetric Key Cryptography in which one key is used for encryption of the data and the second key is used for the decryption of the data.

Symmetric key cryptography is further divided as,

1. Stream Cipher, in which a stream cipher is one that encrypts the plain-text, but it considers only one bit at a particular time.
2. Block Cipher, in which block of plaintext is treated as one entire data stream. This is used to produce the encrypted data having the same length.

II. RELATED WORK

Lokesh S. Khedekar and Prajakta S. Kale (2016) [1] proposed that currently the authentication systems available have strengths and weaknesses. Usage of image as a password has gained interest. They have proposed a technique which shows strengths of QR code image over the authentication system using text.

Nutchanad Taveerad and Sartid Vongpradhip (2015) [2] proposed a new QR code (Color QR code) for increasing capacity of QR codes, so decoding process is different than in the standard QR code. Color QR code reads image color then transfers it to output data. It was found that variety of colors can affect increasing capacity of QR codes and reading accuracy.

J. Galiyawala and Kinjal H. Pandya (2014) [3] proposed a technique that offers 24 times more increase in data capacity as compared to the basic QR code, as there is availability of large amount of color possibilities. The look is same as the basic QR code. It is seen that the technique of multiplexing doesn't change the QR code visually. If this technique is used for digital transmission alone, then the devices, i.e., camera and printing problems can be overlooked.

Sumit Tiwari and Sandeep Sahu (2014) [4] proposed that in the present OMR strategy, sheet-tampering detection is not possible due to which illegal ways of passing exams have increased. The capability of existing system has been enriched due to the proposed technique. OMR is extensively used while conducting exams and hence new method for detection of tampering will help in reducing frauds associated with competitive exams. This method has a huge scope in the future and can be applicable to OMR systems that are practiced in different situations like survey work, attendance system, and many more.

Christina L and Joe Irudayaraj V. S. (2014) [5] proposed an optimized Blowfish Algorithm. Even though larger size of key is safer, the decryption speed is slow. This problem in the Blowfish Algorithm can be overcome if two of the S-boxes are reduced. This will provide increased speed and better data security. The time of execution is reduced to 0.2 milliseconds along with the throughput increasing to 0.24 bytes/milliseconds as compared to the traditional algorithm.

Somdip Dey (2013) [6] proposed that new mark sheet strategy is more effective to reduce use of digital space. The marks that are saved in the sheets cannot be changed because they have a unique encryption using their cipher method. The group at St. Xavier's College, Kolkata, India, has tried to enhance the digital information, which is embedded in the form of QR code, and more important information about the student has been added in the digital format. The TTJSA encryption technique, designed by Nath is a combination of generalized modified Vernam cipher, MSA and NJJSA, for encryption of data in QR Code. After encryption, the data can be embedded in the QR Code.

B. Geethavani, E. V. Prasad and R. Roopa (2013) [7] proposed a technique for securing the data transfer in audio signals by use of discrete wavelet transform. A hybrid technique was derived by combining cryptography and steganography for

message transmission in a safe manner. The plain text is encrypted using Blowfish Algorithm. Finally they suggested that this method is efficient for hiding text in audio files.

Russell K. Meyers and Ahmed H. Desoky (2008) [8] proposed that as the plain text characters is equally distributed and the key is selected at random. It is found that only 12 rounds are needed for security in terms of the Shannon's definition. This cipher and tool be used when it is required to encrypt huge amounts of data with a single key.

Somdip Dey [9] proposed the SD-EQR method, where only text message encryption is shown. Unicode format is used for encrypting, so this method can be used to encrypt any type of the message or a file (picture, video, audio, etc.) and send it to the receiver safely. The QR code brings security to encrypted messages and receiver can access the original message much quickly, just by scanning QR code and decrypting it using software, which uses the above mentioned SD-EQR algorithm.

III. PROPOSED WORK

QR Code Generation and Data Hiding:

Creating a string of data bits is the first step in generating the QR codes . In this case it is going to be the encrypted key which has been given by the Blowfish Algorithm. The string contains the characters which are the part of the original message to be encoded, the University mark sheet in this case, and some information to tell the QR decoder, what kind of QR code it is.

After creating the string, error correction of words is used for the encoding of the QR codes. These codes use the Reed-Solomon (RS) error correction technique. If the size of the encrypted message exceeds 1264 characters, then they appear after 1264 characters, which are used separately to generate another QR code and the above process is continued until the QR code for the input key is generated.

Multiplexing of QR Codes to create Color QR Codes:

The original information which is the encrypted key is divided into ‘m’ parts which are used to create ‘m’ different QR codes. For multiplexing them, 2^m colors are required. QR codes are black and white symbols. Each color makes 1-bit image having pixel value either 0 (for black pixel) or 1(for the white pixel). This entire process can be divided into 3 parts:

1. **Multiplexing with color coding:**

A string of message which is long is split up. Each of these is considered as a separate string to generate the Quick Response code. These are then combined using a procedure which uses color coding. Depending on the individual values of the pixels of the respective QR codes, an index value is generated. This index value is the one which determines the color of the pixel of the resulting multiplexed QR code. Consider the table, in which the first three columns give the value of the color of black and white QR code. For a new combination, a different color is assigned. Normalized values of Red, Blue and Green colors are given in the table. Whenever a certain pattern like 0 1 1 occurs after combining, the Green color is assigned in the position of the colored code.

QR code 1	QR code 2	QR code 3	Index	Red	Green	Blue	Color
0	0	0	0	0	0	0	Black
0	0	1	1	0	0	1	Blue
0	1	0	2	0	1	0	Green
0	1	1	3	1	0	0	Red
1	0	0	4	0	1	1	Cyan
1	0	1	5	1	0	1	Magenta
1	1	0	6	1	1	0	Yellow
1	1	1	7	1	1	1	White

Table 1: Pixel Combination for Color QR Code

2. **De-multiplexing:**

De-multiplexing is the reverse of the initial process. A decoding table is needed to decode the values of the combined codes. . To get the (Red, Green and Blue) values from a multiplexed QR code, separate all the 3 planes. Comparing it with all the combinations will give the original pixel values. This results in the formation of the white and black QR codes which were initially multiplexed. Concatenating the individual messages will give the original long sequence of message.

3. **Generating distinct RGB combinations:**

The task of generating the index value by hand can become extremely time-consuming and inefficient when the number of QR codes to be multiplexed increases. For instance, considering 14 QR codes will result in 16384 distinct combinations, which is not practical. Hence, by generating a matrix which has the color map from any available colorful image can help solve this problem.

The processing time of gets increased if images are more than 10. Hence, if more than 14 images are considered, the de-multiplexing time becomes more than 20 minutes, which is extremely inefficient.

Total Execution Time

Plaintext Size (Bytes)	Key Size (Bytes)	Original Blowfish		Optimized Blowfish		Original Blowfish	Optimized Blowfish
		Encryption Time	Decryption Time	Encryption Time	Decryption Time		
41	8	5.42	0.82	5.00	0.89	6.24	5.90
82	12	6.4	1.51	6.19	1.45	7.91	7.64
47	16	5.42	0.87	5.15	0.86	6.29	6.01
70	20	6.01	1.31	5.89	1.37	7.32	7.26
45	24	5.24	0.87	5.27	0.85	6.11	6.12
72	28	6.30	1.26	6.23	1.31	7.56	7.54
57	36	5.94	1.19	5.77	1.09	7.13	6.86
52	40	5.92	1.07	5.65	0.99	6.99	6.64
49	44	5.91	1.07	5.74	1.03	6.98	6.77
63	56	6.53	1.20	6.36	1.17	7.73	7.53
Average Execution Time						6.83	7.03

Table 2: Total Execution Time = Encryption Time + Decryption Time

The following is the proposed diagram for multiplexing and de-multiplexing. The Data1, Data2….Data n which is going to be encoded in a QR code is the output of the Blowfish Algorithm. This implies that when the CQR code is scanned by a normal scanner, the output will be the encrypted string and not the actual result. This results in enhanced security as well as increased data storage of the QR codes.

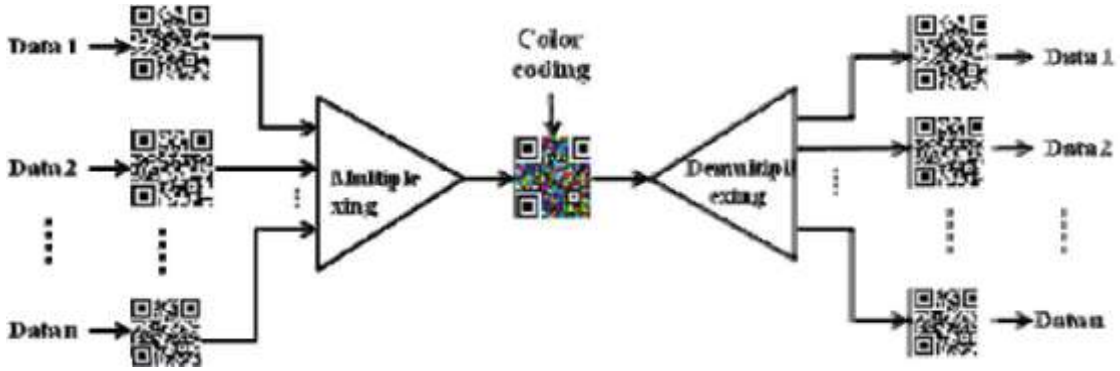

Figure 3: Proposed Diagram for Multiplexing and De-Multiplexing

The Optimized Blowfish Algorithm:

The Blowfish Algorithm (BA) which has been modified is a procedure which has a key length of 56 bytes. It is a Feistel Network which consists of 16 rounds. The protection power of the algorithm is based on the key length. The optimized Blowfish algorithm has the P-array and the 2, 32-bit S-boxes.

Description of optimized Blowfish Encryption Algorithm:
The Sub Key Generation (P-array): Initialize the P array with a string which is fixed. It has 18, 32-bit sub key values. Separate the key string into 18, 32-bits. The first P-array (P1) is XORed with the first 32-bit key (K1), second P-array (P2) value is XORed with the second 32-bit key (K2) and this continues until 18 rounds are completed. It means each of the 18 32-bit P-array values are XORed with 18 32-bit key values. All zero strings are encrypted using the optimized Blowfish algorithm. This is executed in 18 rounds, after which the sub key values are stored in the P-array.

The Preparation of the S-Box: Initialize the S-boxes with a string which is fixed. Each S-box has 256 entries. These S-box values are encrypted using Blowfish algorithm. After that 1st and 2nd S-box values are concatenated and 3rd and 4th S-box values are combined together. Finally the S-box values which are 4 are reduced into 2 S-boxes.

Data Encryption: Data encryption has the F function with 16 rounds. Each round has a key dependent permutation and a key and data dependent substitution. In each round every left half and right half affect each other. The key is affected by every sub key. Figure 4 shows the structure of Blowfish algorithm. This structure is same as optimized Blowfish algorithm.

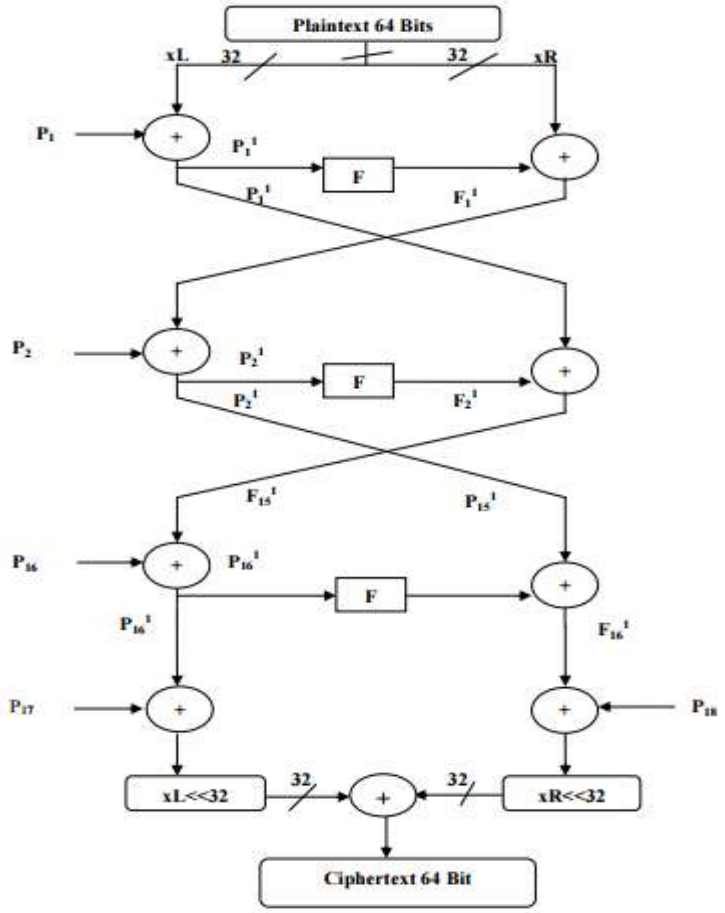

Figure 4: Blowfish Encryption

The F function is irreversible. The function has 4 S-boxes. These 4, 8 bit values are combined using addition and using XOR operation. ,

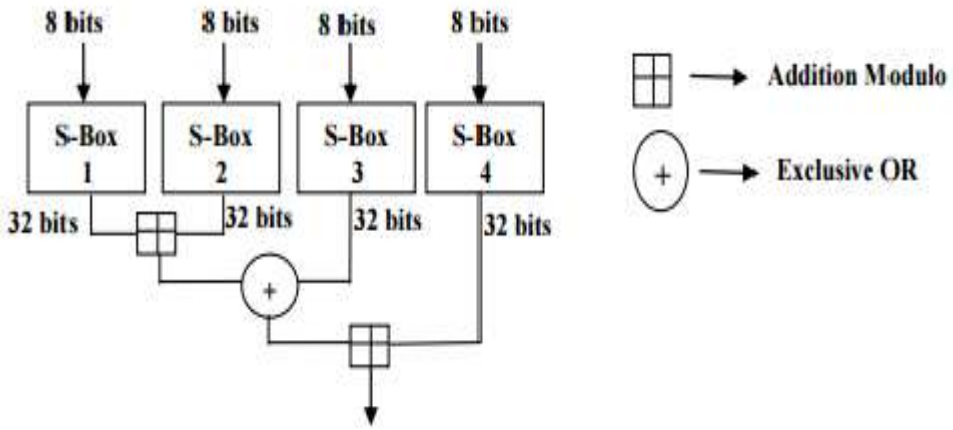

Figure 5: Function F

Modified F Function:

The F Function of the blowfish algorithm uses 4 S-boxes, but in this technique, only two are used. Following Fig 6 shows the modified function.

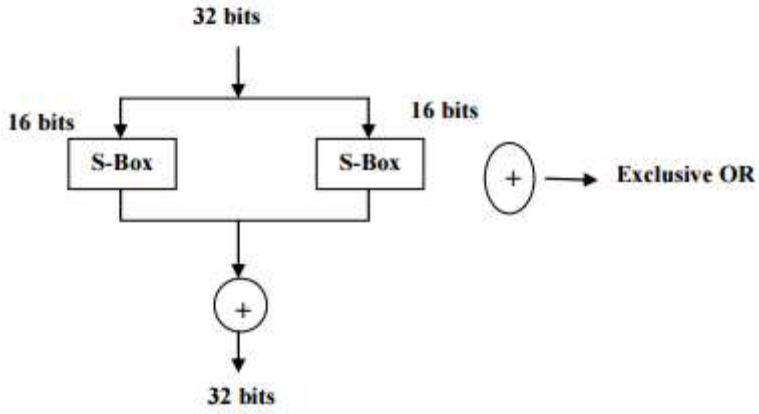

Figure 6: Optimized F Function

The working of optimized Blowfish is illustrated as follows:
1. Initialized the P-array and four S-boxes, in order with a fixed string.
2. Encrypt the key and P-array for preparing the sub keys.
3. Encrypt the S-box values using F function with four S-boxes.
4. Divide the 64-bit input data into two 32-bit halves (left and right). The left half is denoted by XL and right half is denoted by XR.
5. The 32-bit left half XL is XORed with the sub key P1 and assigned into the XL. The XL is fed into the F function.
6. The function F has 2 S-boxes, which split up the 32-bit of input into 2, 16-bit halves and each half is given as an input to each S-box.
   6.1 The first S-box (S1) and second S-box (S2) are added.
   6.2 The resulted bit is then XORed.
   6.3 The optimized F function is: Divide the XR into two 16-bit halves, a and b.
   F (XL) = F (a, b) = (S1 ð S2). Here " ð" is XOR.
7. F (XL) is XORed with XR.
8. Swap XL and XR. It means that the right half becomes the new left half and left half becomes the new right half.
9. After the 17th round the left and right halves are not swapped but XR is XORed with P17 and XL is XORed with P18.
10. XL and XR are finally recombined using the XOR operation.
11. The decryption process is same as the encryption process, but P0, P1... P17 are used in the reverse order. In case of original F function which executes in sequential order, requires two addition operations and one XOR operation. But optimized F-function requires only one XOR operation. To reduce four S-boxes entries into two S-boxes cannot affect the security.

EXPECTED OUTPUT

The result will be encrypted using the above mentioned techniques which will not allow any standard scanner to scan the code and get the result. Any standard QR code if scans the result, will get the encrypted cipher text as the output, as it cannot be decrypted by any standard QR code reader.

We will create an application which will allow the scanning of these QR codes which are generated by the University as they can decrypt the cipher text using the symmetric key. Any kind of changes in the result will change the key, thus making it impossible for our application to decrypt the incorrect key.

Any changes in the QR code will also create an error in the verification of the QR code which is stored in the cloud server or the database of the University, thus avoiding any kind of tampering in the QR code as well.

CONCLUSION

The enhanced Blowfish algorithm is used to encrypt the result sheet of the students. The more the length of the key, the more security it will provide. This takes a toll on the time required to encrypt and decrypt the data. This problem can be solved in the BA, 2 S-Boxes are reduced which increases the speed and provides enhanced security to the data. The benefit of this Blowfish technique is that time is cut down and the throughput is shot up, which is much better compared to the un-optimized algorithm.

IV. REFERENCES

[1] Lokesh S. Khedekar and Prajakta S. Kale, "Strength of QR Code over Design and Implementation of Authentication System", International Conference on Communication and Signal Processing, April 6-8, 2016, India.
[2] Nutchanad Taveerad and Sartid Vongpradhip, "Development of Color QR Code for Increasing Capacity", 2015 11th International Conference on Signal-Image Technology & Internet-Based Systems.
[3] Hiren J. Galiyawala and Kinjal H. Pandya, "To Increase Data Capacity of QR Code using Multiplexing with Color Coding: An example of Embedding Speech Signal in QR Code", 2014 Annual IEEE India Conference (INDICON).
[4] Sumit Tiwari and Sandeep Sahu, "A Novel Approach for the Detection of OMR Sheet Tampering Using Encrypted QR Code", 2014 IEEE International Conference on Computational Intelligence and Computing Research.
[5] Christina L and Joe Irudayaraj V. S., "Optimized Blowfish Encryption Technique", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 7, July 2014.
[6] Somdip Dey, "New Generation of Digital Academic-Transcripts using encrypted QR Code - Use of encrypted QR Code in mark sheets (Academic Transcripts)", 978-1-4673-5090-7/13/$31.00 ©2013 IEEE.
[7] B. Geethavani, E. V. Prasad and R. Roopa, "A New Approach for Secure Data Transfer in Audio Signals Using DWT", IEEE, 2013.
[8] Russell K. Meyers and Ahmed H. Desoky, "An Implementation of the Blowfish Cryptosystem", 978-1 -4244-3555-5/08/$25.OO ©2008 IEEE.
[9] Somdip Dey, "SD-EQR: A New Technique to use QR Codes in Cryptography".

