International Journal of Information Movement Vol.2 Issue IV (August 2017)
Website: www.ijim.in ISSN: 2456-0553 (online) Pages 1-9

SECURING QR CODES WITH CHAOTIC ENCRYPTION SCHEME

Kanchan
M.Tech. Scholar, Deptt. of ECE
Galaxy Global Group of Institutions, Haryana, India
Email:- gatherkanchan@gmail.com
,
Saranjeet Singh
Faculty, Deptt. of ECE
Galaxy Global Group of Institutions, Haryana, India
Email: mail2saranjeet@gmail.com

Abstract: QR Code (abbreviated from Quick Response Code) is the trademark for a kind of matrix barcode (or two-dimensional code) first designed for the car industry. More currently, the device has grow to be popular outdoor the enterprise because of its speedy clarity and huge storage capacity in comparison to conventional UPC barcodes. The code includes black modules (rectangular dots) organized in a rectangular pattern on a white heritage. The statistics encoded may be made of 4 standardized sorts ("modes") of statistics (numeric, alphanumeric, byte/binary, Kanji), or through supported extensions, truely any sort of records. With the rapid growth of the requirement of QR Code transmission on Internet, protection of virtual facts towards unlawful usage becomes increasingly crucial. This paper proposed a chaotic scheme for securing QR Codes, as cumbersome facts ability and excessive correlation amongst pixels in QR Code files, conventional strategies are not suitable for QR Code encryption. Compared with conventional methods (together with AES and DES), chaos-based QR Code encryption schemes have shown advanced performance.

Keywords: Security, QR Codes, Chaotic Encryption

1.0 Introduction

Denso Wave - a subsidiary of the Toyota Group are attributed with the advent of the quick response code as some distance again as 1994 [1]. Originally it was designed to track components inside the vehicle manufacturing enterprise, but its use has grown tremendously. The QR code machine became popular outdoor the car enterprise because of its fast clarity and more garage capability in comparison to traditional UPC barcodes. QR code is the trademark for a type of matrix barcode (or dimensional barcode). A QR code includes black squares organized in a square grid on a white heritage, which can be examine by means of an imaging device such as a digital camera and processed the usage of Reed–Solomon error correction until the photograph can be as it should be interpreted. The required statistics is then extracted from styles which might be found in each horizontal and vertical components of the image. Ordinarily we think about a barcode as a collection of vertical traces. 2D Barcodes or QR Codes are distinctive in that the facts are saved in each instruction and can be scanned vertically or horizontally. Whilst a fashionable 1D Barcode (UPC/EAN) stores as much as 30 numbers, a QR Barcode can store as much as a huge 7,089. It is this big quantity of records that enables links to things like videos, Facebook or Twitter pages or a plethora of other website pages. Moreover, through taking a deeper look at format of QR code modules inside the information vicinity are grouped into phase of 8 modules and the facts is study sequentially. This is proven in fig. 1.1, of which the grey areas stand for facts bits storing facts statistics to hold. In our studies we did not hassle the other elements. What is worth taking note of is that since every eight modules are grouped into a phase and the records is examine phase through segment, if any trade or reordering of unmarried module takes place, the whole eight-bit block phase is rendered or destroyed and causes the facts to be unreadable by using detectors. Although with the assist of mistakes correction in QR code, it's far viable to stay studying the unique records. Yet when the QR code is of low stage of errors correction and it occurs that the QR code is significantly damaged, even modify of a single bit weighs.

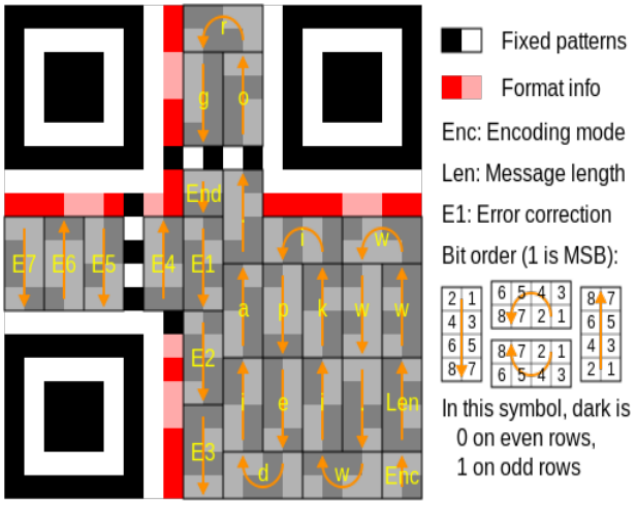

Figure 1.1: Layout of QR code [2]

To summarize the two aforementioned findings regarding modules of QR code, they are:

1. Once upon a QR code is generated, because of model and associated factors, module configuration is fixed.
2. Change or reordering of bit(s) need to be averted, otherwise the predicted statistics dangers of turning into now not detectable or readable. Even a single bit may have impact on other components of statistics. A modern-day era brings QR code encoding and decoding to a higher level. The first factor comes into thoughts to make QR code safer is probably encryption at some stage in encoding and decoding process of a QR code. In maximum cases, intents of the usage of QR code is to benefit most accessibility, which includes guiding potential clients to marketing net websites or gift data of products. Though it is not very common to have encrypted QR code, there may be a want to have such sort of QR code meeting different security specs. Encryption is a procedure of encoding the unique facts in a manner that simplest the anticipated legal recipients can obtain and study it [3]. There are popular procedures in encryption which can be symmetric-key encryption and public-key encryption. The former applies the method that each the sender and recipient share a mystery key for security purposes. While the latter requires a so-known as public key that's used for encrypting statistics to be transmitted and at the recipient side a private key matching the public key is used to decrypt the information acquired. The encryption methods are able to be employed into QR code. In the article written with the aid of Kevin Peng and his colleagues [2], QR code safety standards the usage of encryption have been introduced - Symmetric Encrypted QR code (SEQR) and Public Key Encrypted QR code (PKEQR).

The SEQR made use of symmetric-key encryption and the PKEQR adopted the public-key encryption as described above respectively. Although it's far feasible to apply the two encrypting strategies into QR code, there are sure drawbacks which must now not be unnoticed. Firstly, since keys might be included into the QR code during encoding and interpreting steps, the accuracy of key facts must be guaranteed to a more amplify. This suggests a call for on better error correction degree to ensure that the keys on each of sender and receiver aspects are exactly identical or valid. Secondly, due to the existence of keys, part of statistics space is glaringly occupied for storing such extra records. Thirdly, which won't play so vital position because the formers, is that the computation time to benefit and study a QR code now will become longer. It isn't always so important for that most of users do now not have a strict requirement on encoding or deciphering time of QR code and the growth of computation time in those cases isn't always large. Besides, encryption technology, two of literature reviews furnished us a new vision. The first one mentioned about QR code and watermarking which was to begin with used for copyright. However if judging from every other thing, safety of copyright may be utilized for shielding the integrity of statistics records, this is, to assure the message you get is similar to the one sent. As said inside the article, watermarking was achieved through encoding and decoding greater statistics bits right into a QR code.

The different literature supplied a widespread idea of a way for statistics hiding to maintain the hidden records secretive. The answer given became to utilize each steganography and cryptography [2]. In info, they positioned the image with hidden statistics into a QR code and used a effective encryption algorithm. These articles discussing approximately QR code encoding and deciphering delivered forward sound grounds for in addition development of

QR code security however considering the complexity of some of the algorithms the authors offered and time limit for us, they are to be suggested in encouraged similarly paintings. In our paintings, we might adopt MD5 (Message Digest algorithm five, a broadly used cryptographic hash characteristic generating a 128-bit hash cost to verify statistics integrity) which could be described.

2.0 Related Work

Lorenzi D. et al., (2012) In this paper Digital government is universally gaining acceptance as the public will become more technologically superior. Quick Response codes (QR codes) provide a method to efficaciously distribute many one-of-a-kind styles of records to the general public. We propose a QR code system and a corresponding Smartphone application for the U. S. National Park Service (NPS) with the purpose of imparting a new degree of interactivity for the general public. The attention is on growing a QR code waypoint gadget for park navigation, as well as incentivizing park use via gamification of website attractions. The machine affords multiplied protection for park goers, disseminates statistics more efficiently and correctly, and improves feedback among the NPS and the public [4]. Kapsalis I., (2013) In this paper The 2-dimensional barcodes referred to as QR (Quick Response) Codes are increasing their reputation as they seem in more locations inside the urban surroundings. QR Codes can be taken into consideration as physical hyper-hyperlinks that give the capacity to users to access, via their cellular devices which can be capable of test QR Codes, additional facts positioned in an internet-web page. Apart from marketing, QR Codes had been additionally adopted in different regions which includes the online bills. This development alongside the trend that a number of the customers may additionally comply with which shows to experiment unauthenticated information, including QR Codes positioned in public places, encouraged us to investigate how QR Codes can be used as an assault vector. We first evolved an implementation which tries to brute-force QR Codes with the aid of attacking directly the modules, aiming to retrieve an alternated URL upon scanning the QR Code and after having carried out the module modifications [5]. Vidas T. et al., (2013) In this paper The matrix barcodes called Quick Response (QR) codes are swiftly becoming pervasive in city environments round the arena. QR codes are used to symbolize records, which include a web cope with, in a compact form that may be scanned simply and parsed by way of purchaser cell gadgets. They are famous with marketers due to their ease in deployment and use. However, this technology encourages cell customers to scan unauthenticated data from posters, billboards, stickers, and more, offering a new attack vector for miscreants.

In one test we visually monitored person interactions with QR codes; in the main to study the proportion of customers who scan a QR code however go with now not to visit the associated internet site. In a 2nd test, we allotted posters containing QR codes throughout 139 special locations to look at the wider software of QR codes for phishing. Over our four-week look at, our disingenuous flyers were scanned by 225 folks who eventually visited the associated web sites. Our survey results advise that curiosity is the biggest motivating aspect for scanning QR codes. In our small surveillance experiment, we observed that 85% of folks that scanned a QR code finally visited the associated URL [6]. Kim S. H. et al., (2013) In this paper Internet phishing assaults have been evolving together with the growth of on line transactions at the Internet. MITM (Man-In-The-Middle) phishing is an attack that manipulates authentication and transaction records when an attacker is positioned in among a web server and a user. The possibility of this kind of phishing assault has been posed for a long time, but the threat turned into broadly speaking unnoticed. Since Bruce Schneier added the concept of emasculating two-aspect authentication in 2005, Leung and Jakobsson proposed Control Relay-MITM and doppelganger phishing attacks, respectively. In this paper, we introduce ART (Active Real-Time) MITM phishing assault as an better phishing attack in opposition to above ones. While imparting same UX (User enjoy) of real net server to a consumer, ART-MITM makes all protection solutions which are set up at the person's pc vain and runs computerized attack strategies. To defeat against ART-MITM phishing attack, we recommend a geo-place based QR-code authentication scheme the usage of mobile telephone. The proposed scheme provides convenience, mobility, and safety for the user; as a end result, the scheme may be visible as a practical strategy to such enhanced phishing assaults [7]. Krombholz K. et al., (2014) In this paper QR (Quick Response) codes are two-dimensional barcodes with the ability to encode exceptional varieties of information. Because of their high data density and robustness, QR codes have gained reputation in diverse fields of software. Even though they provide a large variety of advantages, QR codes pose massive security risks. Attackers can encode malicious hyperlinks that lead e.g. To phishing web sites. Such malicious QR codes can be printed on small stickers and update benign ones on billboard advertisements. Although many actual global examples of QR code based totally attacks had been suggested inside the media, handiest little research has been carried out in this field and almost no interest has been paid at the interaction of safety and human-computer interplay. In this work, we describe the manifold use cases of QR codes. Furthermore, we analyze the maximum tremendous attack eventualities with recognize to the specific use instances [8]. Chen J. H. et al., (2014) In this paper In recent years

there was growing interest in the direction of virtual rights. Therefore, this paper proposes a matrix barcode to verify photo copyrights. The copyright text, Quick Response code (QR code), and watermarking techniques are used to attain a hidden identification scheme imposing direct sequence unfold spectrum (DSSS) and modulation of the modified code department more than one access (MCDMA) to cover the QR code statistics. DSSS and MCDMA hash the data and QR code has a robust feature to save you external assaults and destruction of the duvet image. The QR codes records may be effortlessly extracted through cell gadgets. Even if the barcode suffers external harm, a duplicate of the barcode can be hidden within the photograph to easily get better the barcode facts. Compare to the opposite scheme, our method has two blessings: 1) the QR code has common place, fast identity and fault tolerance features, so it's far suitable for copyright safety; and 2) the usage of DSSS and MCDMA strategies to cover facts can offer more protection and fault-tolerant functions [9].

Muthaiah R. M. et al., (2014) In this paper A distinctly efficient approach for hiding data in the back of photographs or another digital media and to lead them to more secure from the intruders is proposed. There are concepts like digital watermarking, photograph steganography, fingerprinting which can be intended for the equal reason however with moderate variations. In this context, cryptography can also be used to make sure security of facts however the distinction between the previous ones and the latter, to be advised in a nut shell, is the idea of steganography keenly specializes in preserving the existence of a message secret while the cryptographic strategies revolves around retaining the contents of the message secret and safe from the intruder. There are safety threats when the above said strategies are used in my opinion to shield and preserve data mystery. Hence we endorse a method where we cover the facts at the back of any digital media, here behind an picture and to have its existence secretive, we positioned the picture with hidden information into a QR code and use a powerful encryption algorithm [10]. Dobrescu A. et al., (2015) In this paper Web technologies and tools have seen an improved development in the final years bringing introduced cost to the advertising and marketing activity carried out at business enterprise level. They have continually sought to facilitate manufacturing, distribution and verbal exchange procedures. Moreover, the applications evolved online have enabled the verbal exchange with the consumers and facilitated the short sending of the data concerning the goods commercialized. The emergence and improvement of QR codes in the market place enabled the advertising and marketing specialists to speak less difficult with their goal public as these codes assist them ship quite a number information on the products /offerings commercialized, promotions, competitions, events held, etc. [11].

3.0 Proposed Work

Cryptography is ready correspondence in the location of an adversary. It joins numerous issues like encryption, test, and key task to call a pair. The discipline of current cryptography gives a theoretical stronghold targeted round which one can fathom what actually these problems are, the exceptional approach to assess traditions that infer to light up them and a way to accumulate traditions in whose safety one may have conviction. Advanced automated advances have made media records with the aid of and big available. Starting overdue, media procurements get crucial in practice and along those strains safety of sight and sound statistics has gotten trendy issue. The principal problems figuring out with the problem of encryption has been inspected and furthermore an define on picture encryption techniques focused on chaotic strategies had been overseen in the gift correspondence. The chaotic QR Code encryption might be made by way of the usage of homes of chaos along with deterministic elements, erratic behavior and non-instantly trade. This thought prompts exercises that can within the period in-between provide protection limits and a widespread visual test, which may be suitable in more than one demand. Automated pix are for the most component used as a piece of various orders, that is a part of navy, genuine and beneficial frameworks and these procurements want to control get entry to pix and deliver the means to verify uprightness of QR Codes. The maximum aged and fundamental trouble of cryptography is cozy verbal exchange over a shaky channel. Party A wishes to ship to accumulating B a thriller message over a correspondence line, which can be tapped by using an enemy. The late trends in engineering, in particular in machine industry and correspondences, approved probable first rate commercial enterprise for appropriating computerized interactive media content thru the Internet. Then once more, the multiplication of superior data, picture dealing with apparat uses, and the general accessibility of Internet get entry to have made a perfect medium for copyright misrepresentation and wild appropriation of media, as an example, photograph, content material, sound, and characteristic content. An exchange good sized take a look at now's the manner by which to relaxed the certified innovation of media substance in sight and sound structures. To control the specialized difficulties, the two vast image protection advances are underutilize: (a) QR Code encryption procedures to give end-to-end security when dispersing advanced substance over a mixture of disseminations systems, and (b) watermarking systems as an instrument to accomplish copyright insurance,

proprietorship follow, and verification. A novel QR image encryption algorithm based on Chaotic Map is proposed. To overcome fundamental drawbacks in the widely used one-dimensional chaotic system, our proposed scheme presents good encryption system with large key space. We perform some security analysis to prove that the key space of the new algorithm is sufficiently large thus making the brute-force attack infeasible. Simulation results demonstrate that satisfactory performance (sensitivity, security, and speed) is achievable in our proposed algorithm. Results show that our QR encryption algorithm outperforms current image encryption algorithms in terms of security, sensitivity and speed. Hence, based on the achieved results, we can strongly claim that the proposed scheme successfully overcomes the limitations in current one-dimensional chaotic image encryption system, and best suits the real-time image encryption and transmission applications. We show that the QR encryption procedure is analytical and hence time-saving. Moreover, the proposal demonstrated has huge key space and robust against noise attack. The feasibility and effectiveness of the proposal have been demonstrated by numerical experiments. In this paper, the waft research endeavors in photo encryption methods centered around chaotic plans are tested. Interactive media protection most of the time is given by using a machine or a hard and fast of techniques used to comfortable the sight and sound substance. These systems are intensely targeted round cryptography and that they empower both correspondence security, and safety towards robbery (Digital Rights Management and watermarking), or both. The encryption set of rules proposed in this is based totally on permutation–diffusion structure. The initial value x0 and the manipulate parameter of skew tent map are used as mystery key. The permutation step is defined With Wang's diffusion scheme, step five in encryption makes the diffusion key stream not most effective associated on the key however also the obvious QR Code. For a gray QR Code of size M×N, we treat its data as a one-dimensional vector P= {p0,p1,..,pMN-1}. The algorithm can be described as follows (take 256 gray-scale QR Code as an example).

4.0 Encryption algorithm:

Step 1:
Iterate the skew tent map x_{i+1}=F (x_i). Generate a P-box T and shuffle the values in P by T to get P'.
Step 2:
Let i←0.
Step 3:
Obtain an 8-bit random code d_i according to the following formula:
d_i = mod. $(floor(x \times 2^{48}), 256)$ (3.1)
where x is the current state value of the skew tent map system.
Step 4:
Compute the corresponding pixel data of the cipher-QR Code by using the values of the currently operated pixel and the previously operated pixels, according to the following formula:
$c_i = p'_i \oplus mod(p_{i-1} + d'_i, 2^8)$ (3.2)
Where + is bit wise XOR operator and c_i is the output pixel data. One may set the initial valuep'_{-1} as a constant. The inverse form is
$p'_i = c_i \oplus mod(p_{i-1} + d'_i, 2^8)$ (3.3)
Step 5:
Compute k according to the formula:

K= 1 + mod$(c_i, 2)$ (3.4)
Then, iterate the skew tent map x←F(x) for k times
Step 6:
Let i←i+1, return to step 4 until it reaches MN.

Decryption algorithm:

The decryption procedure is similar to that of the encryption process in the reverse order.
Step 1:
Generate a P-box T by skew tent map according to the x_0 and p.
Step2:
Obtain P' = $\{p'_0, p'_1, \ldots, p'_{MN-1}\}$ from C=$\{c_0, c_1, \ldots, c_{MN-1}\}$. Perform the reverse operations to remove the effect of diffusion. All operations are the same as steps 3 - 6 in the encryption process.

Step 3:
Perform the reverse operation to remove the effect of permutation by using the P-box T.

5.0 RESULT AND ANALYSIS

In cryptography, encryption is the process of encoding messages (information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plain text) is encrypted using an encryption algorithm, turning it into an unreadable cipher text.

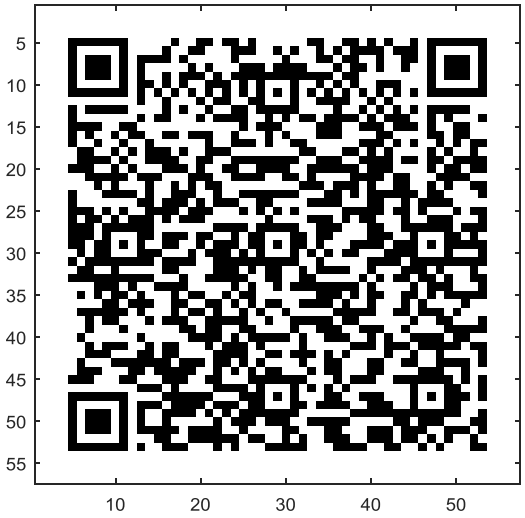

Fig 4.1: QR Code Generated with message = 'Secret Message for QR Code'

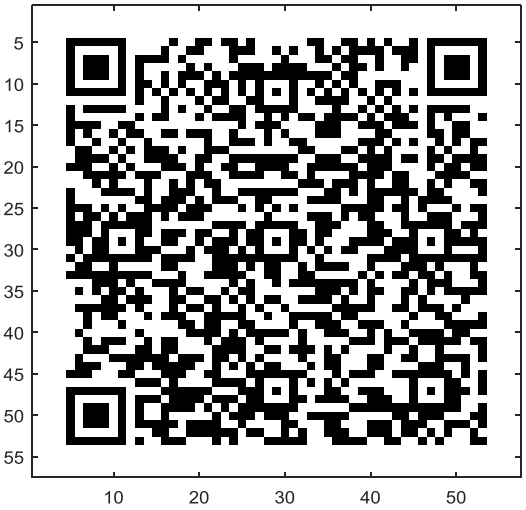

Fig 4.2: QR code generated with message = ' www.mathworks.com'

QR Code generated with information message is shown here. As the information increases, the black dots area also increases
under the encryption. These information can be assessed by using and QR code reader or any other similar device etc.

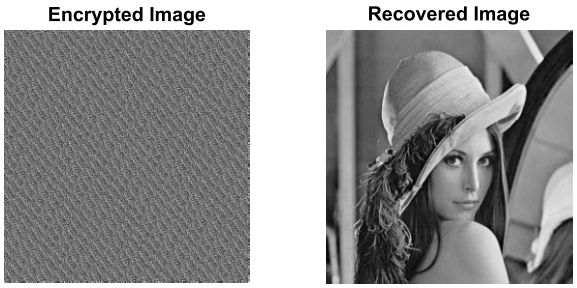

Fig 4.3: Decryption of the input image with Exact code

Decryption of the input image is shown here with the exact code. If the decryption is processed with the wrong code then input image will not be recovered and the attack will not be successful

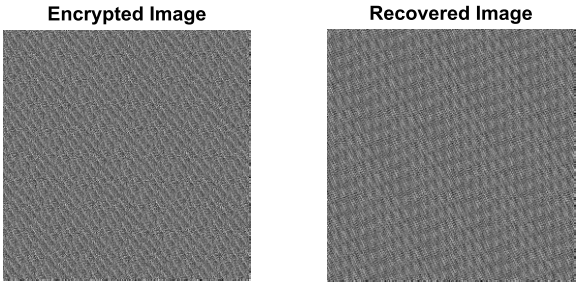

Fig. 4.4: Decryption of the input image with wrong code

Decryption of the input image is shown here with the wrong code and the output image will be just like the encrypted one.

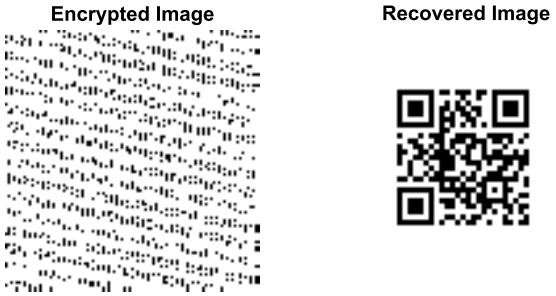

Fig. 4.5: Decryption of the QR code with Exact code

In the similar manner, encryption and decryption of QR code can be processed to get the required image depending upon the right or wrong code. Here decryption of QR code is shown with the exact code and the recovered image is a QR code.

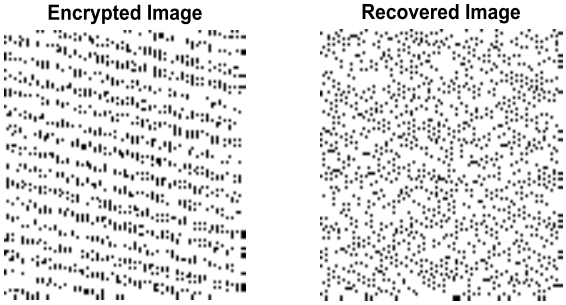

Figure 4.6: Decryption of the QR code with wrong code

Decryption of QR code with wrong code is shown here and the recovered image is just like encrypted one providing no information.

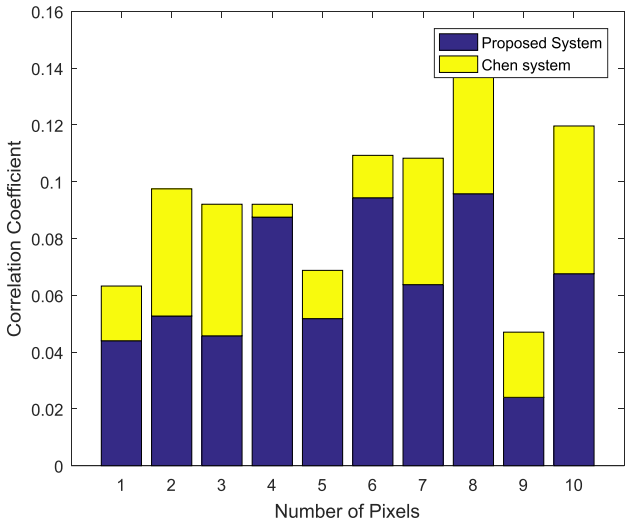

Fig 4.7: Comparison of Correlation Coefficient (CC) of Encrypted counterpart, for Encrypted counterpart the CC must be lower indicating lower probability of attacks.

Here comparison of Correlation Coefficient of proposed system and Chen system is shown. To avoid any kind of attack, the value of Correlation Coefficient must be as small as possible for the encrypted part. Lower value of Correlation Coefficient indicated lower possibility of attacks.

6.0 Conclusion and Future Scope

Here, a singular QR photograph encryption algorithm primarily based on Chaotic Map is proposed. To triumph over fundamental drawbacks inside the broadly used one-dimensional chaotic system, our proposed scheme offers appropriate encryption device with big key space. We perform some protection evaluation to show that the key space of the brand new algorithm is satisfactorily huge hence making the brute-force assault infeasible. Simulation results reveal that best overall performance (sensitivity, security, and pace) is practicable in our proposed algorithm. Results display that our QR encryption algorithm outperforms current photograph encryption algorithms in phrases of protection, sensitivity and pace. Hence, primarily based on the achieved consequences, we will strongly claim that the proposed scheme correctly overcomes the limitations in cutting-edge one-dimensional chaotic image encryption gadget, and first-class fits the real-time image encryption and transmission packages. We display that the QR encryption manner is analytical and therefore time-saving. Moreover, the suggestion has also been proven to have large key space and to be strong towards noise attack. The feasibility and effectiveness of the thought have been established by way of numerical experiments.

7.0 References

[1]. Narayanan A.S., “QR Code and Security Solution”, International Journal of Computer Science and Telecommunications, Vol. 3(7), July 2012.
[2]. Peng K., Sanabria H., Wu D. and Zhu C., “Security Overview of QR Codes”, 6.857 Computer and Network Security, Massachusetts Institute of Technology, 2014. [Online] URL: https://goo.gl/kRGp8x.
[3]. Mao Y. and Wu M., "A Joint Signal Processing And Cryptographic Approach To Multimedia Encryption." IEEE Transactions on Image Processing, Vol. 15(7), pp. 2061-2075, 2006.
[4]. Lorenzi D., Shafiq B., Vaidya J., Nabi G., Chun S. and Atluri V., "Using QR Codes For Enhancing The Scope Of Digital Government Services", Proceedings of the 13th Annual International Conference on Digital Government Research, Association for Computing Machinery, pp. 21-29, 2012.
[5]. Kapsalis I., "Security Of QR Codes", Norwegian University of Science and Technology, 2013.

[6]. Vidas T., Owusu E., Wang S., Zeng C., Cranor L. F. and Christin N., "QRishing: The Susceptibility Of Smartphone Users To QR Code Phishing Attacks." International Conference on Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 52-69, 2013.
[7]. Kim S. H., Choi D., Jin S. H. and Lee S. H., "Geo-Location Based QR-Code Authentication Scheme To Defeat Active Real-Time Phishing Attack." Proceedings of the 2013 ACM workshop on Digital identity management, Association for Computing Machinery, pp. 51-62, 2013.
[8]. Krombholz K., Frühwirt P., Kieseberg P., Kapsalis I., Huber M. and Weippl E., "QR Code Security: A Survey Of Attacks And Challenges For Usable Security." Human Aspects of Information Security, Privacy and Trust, Springer International Publishing, pp. 79-90, 2014.
[9]. Chen J. H., Chen W. Y. and Chen C. H., "Identification Recovery Scheme Using Quick Response (QR) Code And Watermarking Technique." Applied Mathematics & Information Sciences 8, No. 2, pp. 585-596, 2014.
[10]. Muthaiah R. M. and Krishnamoorthy N., "An Efficient Technique For Data Hiding With Use Of QR Codes-Overcoming The Pros And Cons Of Cryptography And Steganography To Keep The Hidden Data Secretive." International Journal of Computer Applications, Vol. 100(14), pp.1-5, 2014.
[11]. Dobrescu A., "Implications Of QR Codes For The Business Environment." Calitatea 16, No. S3:166, 2015.