iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** X **Month of publication:** October 2023

DOI: https://doi.org/10.22214/ijraset.2023.56117

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

Implementing Number Theory in Visual Cryptography for Secure Online Transactions using QR Codes

Agasthiya Reni Selvasingh[1], Manikandan K M[2]
[1]*M.Sc Mathematics,* [2]*Assistant Professor and Head, Department of Mathematics, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India.*

Abstract: ***In this modern world, due to the excessive availability of the Internet, it is extremely easy for people to communicate and share multimedia contents with each other. Moreover, Online Transactions has also been widely developed, in which secure means of data transfer play the major role. At the same time, secure transfer of personal and copyrighted data has become a critical issue. Visual cryptography (VC) is a useful tool for securing data (i.e. images, texts) that contain sensitive information. As a subset of secret sharing, VC has got importance for its security mechanism, which takes into account both image processing and cryptography. To achieve this goal, we manipulate quick response (QR) code as a container. QR codes generated by a certain system can carry its ordinary message in addition to the secure data. Anyone can read the message, but the secure data can only be obtained using a secret key. In this paper, a specified field of Mathematics, Number Theory is implemented in the concepts of VC for the secure online transactions which is achieved using QR codes.***

Keywords: Number Theory, Visual Cryptography, Image Processing, Encrypting, Decrypting, Online Transactions, Secret Sharing Scheme, QR codes.

I. INTRODUCTION

Secret sharing of data involves visual cryptography scheme (VCS) which was first proposed by Naor and Shamir in 1995. Based on the original definition of a (k, n)-VCS, a secret image is distributed into n shares in which no secret information will be revealed with possession of fewer than k shares. However, when k or more shares are superimposed, the secret can be easily decrypted. Recently, VCS was developed rapidly and has made great progress in many aspects. All studies contribute a lot to the practical applications of VCS. In earlier times, the only downside of VCS is that the shares in these schemes are meaningless and easily arouse suspicion of some potential attackers when distributed via a public channel. Therefore, the extended VCS (EVCS) was developed as it generates meaningful shares instead of random images. By adding some extra columns into the basic matrices, Wang et al. (Wang, Yi, & Li in 2009) designed a (k, n)-EVCS with poor contrast of shares, to improve its visual performance. And other studies have also been attempted for better results. Nevertheless, the camouflage effect of these shares in VCS schemes was still unsatisfactory since there have been many noisy visible points.

In the time being, Quick Response (QR) code was developed by the Japanese Denso Wave Company. QR code is a two-dimensional code which has been adopted as a universal specification performed by ISO (2006). Such a popularized intelligent terminals, QR codes have been widely used in various fields such as information storage, mobile payment and electronic tickets. For any QR code, we cannot acquire its message by human vision since it is full of dark and light modules which are randomly distributed. These meaningless appearance were similar to the image characteristic of VCS shares. Thus, QR code has considered as the better choice for the mask of VCS share. Therefore, the field of investigations of the VCS and QR codes combinations have attracted considerable attention. In the beginning, QR codes were embedded as a parts of shares to authenticate a VCS by Wang, Liu, & Yan in 2014. Later, a continuous-tone VCS was developed by Yang, Liao, Wu, & Yamaguchi in 2016, where the colour of a secret module was determined by the greyness of black dots. Subsequently, an EVCS based on QR codes was presented with two-level information storage by Liu et al. (Liu, Fu, & Wang, 2016). In this scheme, various standards were to be followed such as a proper scanning, distance and angle are strictly required to decoding the shares, which significantly increases the inconvenience of its practical applications. A (k, n)-EVCS was successful with the help of some concepts of Number Theory. In this method, a secret image to be shared is compressed and encrypted. The process of encryption includes distributing the secret module to n-shares (VCS) and QR code combinations [1].

This simultaneous image compression and encryption technique is an attempt to provide a remedy for both the bandwidth utilization and the encryption problems at the same time. In this paper, Number Theory based Image Compression Encryption (NTICE) is used. NTICE is an algorithm that employs Chinese Remainder Theorem (CRT) in order to generate and solve congruencies and hence obtain simultaneous image compression and encryption.

II. NUMBER THEORY

A. Congruences

Congruence is nothing but a statement about divisibility. It is simple yet enormously useful and powerful to the study of number theory. Consider 'n' is a positive integer, then integers 'a' and 'b' are congruent 'modulo n', $a \equiv b \ (mod\ n)$, if they have the identical remainder on division by n.

B. Chinese Remainder Theorem (CRT)

The CRT render a distinctive solution to various linear congruences with co-prime moduli. In its basic form, the CRT will regulate a number 'n' that, when divided by some given divisors, leaves remainders. The CRT is focused on the solution of linear and modular congruences.

1) Statement

Consider a system of congruences to different moduli:
$x \equiv a_1 \ (mod\ m_1), x \equiv a_2 \ (mod\ m_2), \dots, x \equiv a_r \ (mod\ m_r)$ and if each pair of moduli are relatively prime,
$g.c.d\ (m_i, m_j) = 1$ where $i \neq j$. The system has exactly one common solution modulo M= m_1 m_2 ... m_r, and any two solutions are congruent to one another modulo M.
The CRT can be applied to increase the efficiency by making use of relatively small numbers in most of the calculation. The CRT has been a useful tool in applications of number theory to various fields [2].

2) Merits of CRT

a) Enlarged efficiency in machine computation.
b) Reduced memory and refined hardware requirements.
c) Depletion in space requirement for storage of data because large numbers are converted into relatively smaller ones by solution of linear congruencies.
d) Use of simple arithmetic operations like addition, subtraction, multiplication, division and hence execution of Million Instructions per Second (MIPS) is attainable.
e) Faster computation process and hence depletion in processing time.
f) Widespread application in cryptography, secure transmission of codes and signals in military and defence applications.

C. Number Theory based Image Compression Encryption

The CRT solves the system of linear congruences $a \equiv b \ (mod\ n)$, reducing it to a set of $x \equiv a \ (mod\ \ n_i)$, where $n_1, n_2 \dots \ n_i$ are prime factors of n. This concept of the CRT is used in the NTICE algorithm.

1) Flow Chart

The flow diagram of the NTICE based image coding system is shown in Figure.1

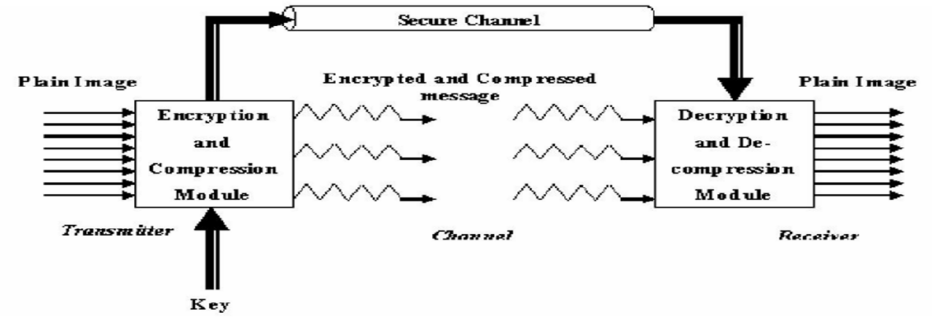


Figure 1. Block Diagram of the NTICE Scheme

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

2) Algorithm Procedure

The images are generally represented in the form of $N \times M$ matrix. In colour image coding applications the colour spaces, namely red, green and blue in 24 bits per pixel (bpp) RGB scale, of 8 bpp each are compressed separately as in the grey scale image.

An image of size $N \times M$ is taken and is fragmented into blocks of size $1 \times K$. Every pixel $r[i]$ in the block is divided by 16 to generate two half pixels of 4 bits each. This procedure is called thresholding.

$$a[i] = r[i]/16, where\ i = 1\ to\ K$$
$$a'[i] = r[i] mod\ 16, where\ i = 1\ to\ K.$$

Thus the input image is appraised as a sequence of half pixels $a[l, 2, \ldots K], a'[1,2, \ldots K]$ and the key sequence is a set of relatively prime numbers given by $n[l, 2., K] > a[i]\ and\ a'[i]$.

- Image: a[1, ..., K], a'[1, ..., K] → block of half pixels
- Key: n[1,..., K] → set of relatively prime integers

Now the Coefficients of the CRT are obtained by generating N for each key value using P, where P is the product of all the keys considered.

$$N[i] = P\ /\ n[i]\ where\ P = \prod n[i].$$

Now the linear congruences are bring about by using the equation

$$N[i] * x[i] \equiv 1\ (mod\ n[i])$$

Where $x[i]$ satisfies the above given congruency and

$$C[i] = N[i] * x[i].$$

These stages are sustained on prior to transmission, the values of C[i] can be generated once the key is decided; hence they are calculated and stored in the system to be used during transmission.

For the transmission of the image, the value of TR is resolved for each block of K half pixel values.

$$TR = \sum C[i] * a[i]\ (Mod\ P) - Cipher\ Text\ (Q), \quad where\ Q\ is\ a\ quotient$$
$$TR' = \sum C[i] * a'[i]\ (Mod\ P) - Cipher\ Text\ (R), \quad where\ R\ is\ a\ Remainder$$

This is the important step of the algorithm as it make sure simultaneous encryption and compression. At the reception part, the K half pixel values are generated from the single value TR and TR'.

$$ar[i] = TR\ (mod\ n[i]) - Plain\ Text\ (Q), \quad where\ Q\ is\ a\ quotient$$
$$ar'[i] = TR'(mod\ n[i]) - Plain\ Text\ (R), \quad where\ R\ is\ a\ Remainder$$

The pixels are then reconstructed from the half pixels as

$$s[i] = ar[i] * 16 + ar'[i]$$

3) Advantages of NTICE algorithm

a) Employment of simultaneous encryption and compression.
b) Enhanced level of security.
c) Optimum compression ratio.
d) Zero latency at the receiver.
e) Decryption is substantially simplified than encryption.
f) Simple computational or number crunching steps.
g) Applicable for diverse applications like remote sensing, biomedical imaging.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

III. IMPLEMENTING PROCESS

A. Algorithm

For secure online Transactions, two images can be merged so that when an intruder tries to intercept the image, it is not knowledgeable to him. This concept can be implemented on the NTICE algorithm to advance its encryption levels. The algorithm for the application is [5]:

1) *Step 1:* Obtain the pixel values of both the images.
2) *Step 2:* Merge the Most Significant bit (MSB) and Least Significant bit (LSB) pixel to obtain half byte words.
3) *Step 3:* These 4 bit values are then given as inputs to the NTICE Scheme. Figure. 2
4) *Step 4:* The encrypted and compressed pixels are transmitted.
5) *Step 5:* On reception the key is used to retrieve the pixel values.
6) *Step 6:* The MSB and LSB bits are re-arranged in order to obtain the original images.

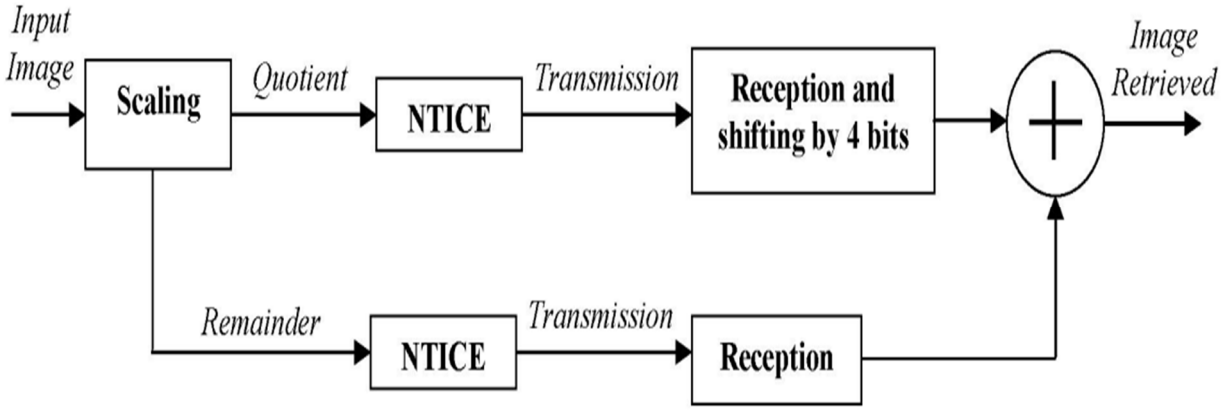


Figure 2. Transmission and Reception

IV. VC FOR QR CODES

The association between VC and QR code is a natural choice, considering that QR code is so widely used nowadays as an information carrier. Recent work is restricted to utilizing the error correction capabilities of the QR code to hide a secret QR code. Utilizing other redundancies in QR code should be a possible direction to explore, including redundancy of un-utilized code words and redundancy of colors. Utilizing the color QR code to design color VC is also a topic worth exploring [4]. Using a color space, more freedom may exist that one can utilize to improve the perceptual quality.

Rani at.al. Proposed a secure system in which they combined between steganography and QR codes [12]. Steganography is considered as the first line of defense in information security as it hides a secret message inside an innocent looking file (container) to transfer the payload under the adversary's nose without noticing it. Their system consists of two parts. The first one is creating a QR code of the encrypted secret message. The second one is hiding the colored image inside a generated QR code. The concealing process does not generate a visible image distortion and produce a very minimal bit error rate.

Barrera et.al. Implemented a system that utilize QR codes in optical encryption as containers [13]. They choose QR codes as containers in their system because of their tolerance to noise. In addition, QR codes are easy to read using mobile phones' camera. The results of the proposed method show that their system is more prone to noise compared to normal optical encryption.

Dey et. al. suggested a steganographic system which is based on a randomized intermediate QR host that is embedded with an encrypted secret message [14]. First, the secret message is encrypted then concealed in a QR code. After that, the QR code is camouflaged inside an image. Using double encryption and embedding techniques makes the system hard to break. But on the other hand, it makes the system less time-efficient.

V. SECURE ONLINE TRANSACTIONS

In this technological world, online transaction plays the major role in the transaction methods due to the widely use of e-commerce. Such transactions include online banking and payment on an e-commerce platform, payment through scanning a QR code, and payment using an online social network App. For these transactions to be secure, we need to ensure that both the hardware and the software are secure (i.e.) there exists no Trojan horses unknowingly in the devices.

A Trojan horse is a malicious program, in hardware or in software, residing in a client or a server, trying to compromise the security of a computer system or a communication system. However, considering the diverse sources of Apps and software's installed on a computer or cell phone, one cannot guarantee that their device is Trojan-free. Using such insecure devices causes our transactions insecure. This maybe because, a Trojan horse may monitor all messages from bank sever to a user's device and may be able to modify these messages. Furthermore, there are two habitual attacks on the communication between the bank sever and the client computer.

A. (2,2) – VCS algorithm using QR codes

This design makes use of the visual cryptography scheme (VCS) algorithm, which is used to secure transactions between users. It is based on a (2, 2) VCS, where two shares are generated and the two shares are required to be stacked to present the original image.

The algorithm itself is bidirectional, such that the input can be encrypted at one end, then once again decrypted at the other. Both the encryption and decryption of images, the QR codes, are done at the server's side for increased security as to not allow any possibility of tampering at the client's side. The service starts with a merchant requesting a payment to be commenced providing a specific amount to be expected. There are various application that creates the accustomed QR code with provided merchant information from the server itself, feeds it into VCS, and transports one of the produced shares to the merchant in the form of a QR code which is to be scanned. The other share will be kept in the server [18]. Scanning the QR code will prompt the server to acquire the related twin share, combine both shares, and complete a successful transaction.

The Figure. 3 presents the process of generating two shadows from a QR code while the right side of the same figure shows the process of verifying a QR code upon scanning.

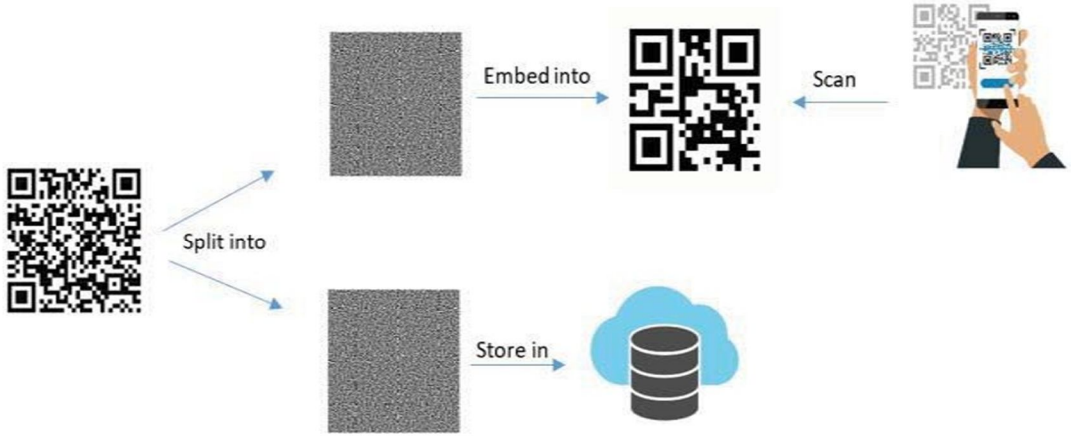


Figure 3. Block Diagram of the (2, 2) – VCS using QR Codes.

VI. CONCLUSION

In this paper, the implementation of Number Theory in VC for secure online Transaction using QR codes was discussed. These QR codes have been enormously used in recent years since they speed up the payment process and provide users with ultimate convenience. However, QR-based online payment systems are vulnerable to different types of attacks. Hence, transaction processing must be secured to protect the integrity and confidentiality of every payment process. Moreover, the online payment system need to provide authenticity for both the sender and receiver of each transaction. In this paper, the online transaction security of the proposed QR-based system is provided using visual cryptography. This algorithm provides a simple and user-friendly interface for users to carry out payment transactions in user-friendly secure environment. The online payment technology has evolved greatly in businesses and has vastly enhanced customer experience. As the payment process is invisible to the user, technological substitutions are looking for ways to make the payment process faster, more secure, and innovative.

In online payments, no mistakes can be afforded as the convenience of online payment systems has also opened up an extensive set of cyber-attacks. These attacks include data theft, denial of service, fraud and forgery, among others. The security of the proposed systemis unique in the sense that it adapts a one-in-all algorithm to provide the needed security services: confidentiality, integrity, and authentication, using visual cryptography embedded through Number Theory.

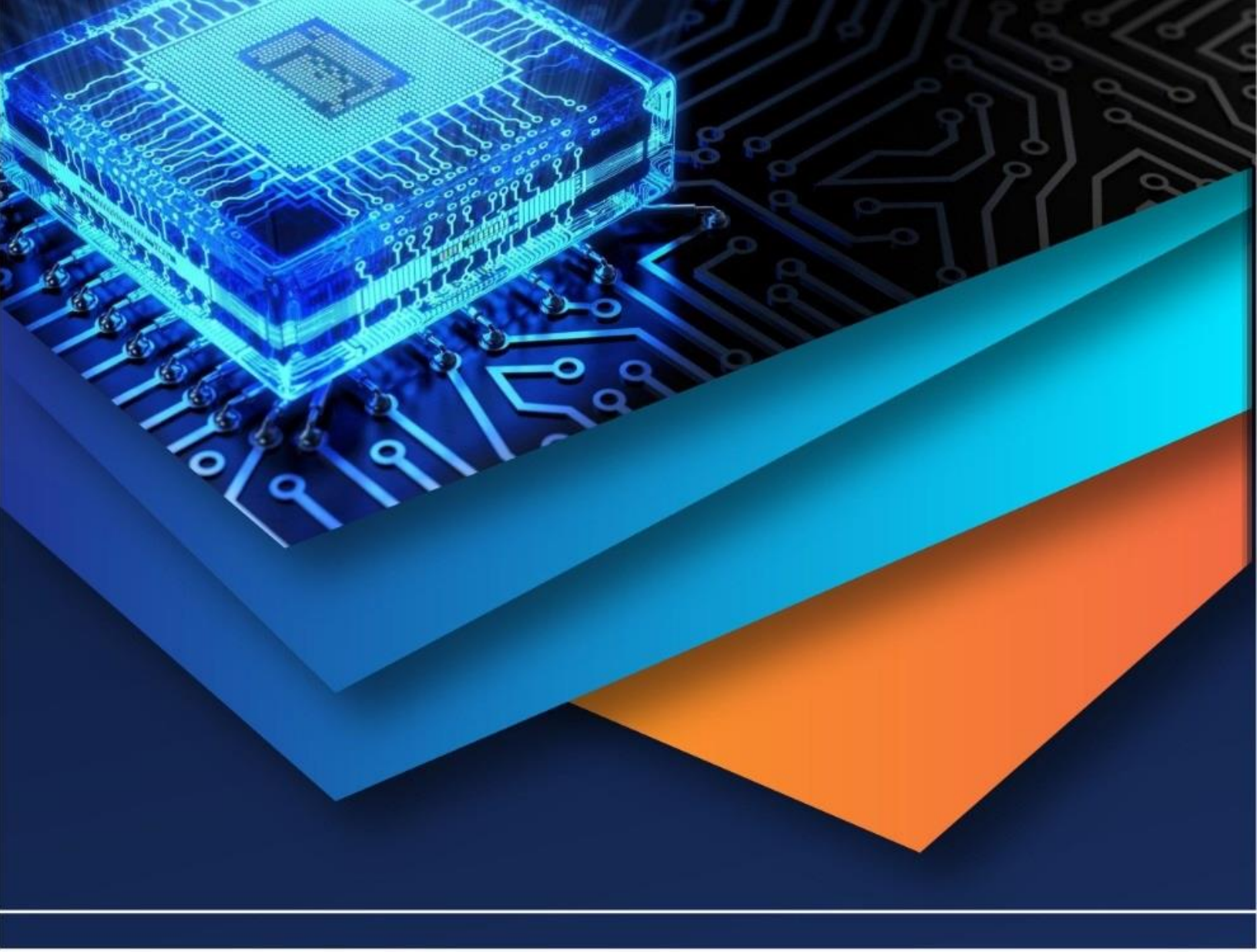
VII. FUTURE WORKS

The algorithm can be extended to higher levels of encryption and compression by increasing the key length. Also, specialized hardware can be developed for the transmission and reception modules, to calculate the computation time and to deploy Number Theory based Image Compression Encryption.

In this scheme, various standards were to be followed such as a proper scanning, distance and angle are strictly required to decoding the shares, which significantly increases the inconvenience of its practical applications. In future works, these standards can be removed by various algorithms.

REFERENCES

[1] Yuqiao Cheng, Zhengxin Fu, Bin Yu, Gang Shen, General Construction for Extended Visual Cryptography Scheme Using QR Codes, International Journal of Digital Crime and Forensics Volume 11, Issue 1, January-March 2019.
[2] Residue number system, http://en. wikipedia. orglw/index.php?title=Residuenumber_system&oldid= 71288485.
[3] Vikram Jagannathan, Aparna Mahadevan, R. Hariharan and E. Srinivasan, Number Theory Based Image Compression Encryption and Application to Image Multiplexing, IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, 2007. Pp 59-64.
[4] Andr, P.S., Ferreira, R.A.S.: Colour multiplexing of quick-response (QR) codes. Electron. Lett. 50(24), 1828–1830 (2014).
[5] Vikram Jagannathan, Aparna Mahadevan, Hariharan R., Srinivasan E., "Simultaneous color image compression and encryption using number theory", Proceedings of ICIS 05, 2005, pp. 1.
[6] Yan, B., Xiang, Y., Hua, G.: Improving the visual quality of size-invariant visual cryptography for grayscale images: an analysis-by-synthesis (AbS) approach. IEEE Trans. Image Process. 28(2), 896–911 (2019).
[7] Bin Yan, Yong Xiang, Guang Hua, Improving Image Quality in Visual Cryptography, Signals and Communication Technology, more information about this series at http://www.springer.com/series/4748, ISSN 1860-4862 ISSN 1860-4870 (electronic) Signals and Communication Technology ISBN 978-981-13-8288-8 ISBN 978-981-13-8289-5 (eBook).
[8] Cheng, Y., Fu, Z., Yu, B.: Improved visual secret sharing scheme for QR code applications. IEEE Trans. Inf. Forensics Secur. 13(9), 2393–2403 (2018).
[9] Nisha, S., Madheswari, A.N.: Prevention of phishing attacks in voting system using visual cryptography. In: 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), pp. 1–4 (2016).
[10] Yan, B., Chen, N., Yang, H.M., Hao, J.J.: Local blackness preserving visual cryptography for grayscale secret images. J. Inf. Hiding Multimed. Signal Process. 9, 370–382 (2018).
[11] Yan, B., Xiang, Y., Hua, G.: Improving the visual quality of size-invariant visual cryptography for grayscale images: an analysis-by-synthesis (AbS) approach. IEEE Trans. Image Process. 28(2), 896–911 (2019).
[12] S. R. M. Mary and E. K. Rosemary, ‘‘Data security through QR code encryption and steganography,’’ Adv. Comput., Int. J., vol. 7, nos. 1–2, pp. 1–7, Mar. 2016.
[13] J. F. Barrera, A. Mira, and R. Torroba, ‘‘Optical encryption and QR codes: Secure and noise-free information retrieval,’’ Opt. Express, vol. 21, no. 5, pp. 5373–5378, Mar. 2013. [Online]. Available: http://www. opticsexpress.org/abstract.cfm?URI=oe-21-5-5373
[14] S. Dey, K. Mondal, J. Nath, and A. Nath, ‘‘Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted secret message: ASA_QR algorithm,’’ Int. J. Mod. Educ. Comput. Sci., vol. 4, no. 6, pp. 59–67, Jun. 2012.
[15] S. Tiwari, "An Introduction to QR Code Technology," 2016 International Conference on Information Technology (ICIT), Bhubaneswar, 2016, pp. 39-44.
[16] Kamal, Sawsan & Ameen, Basheer. (2016). A New Method for Ciphering a Message Using QR Code. Computer Systems Science and Engineering. 6. 19-24.
[17] M. F. Tretinjak, "The implementation of QR codes in the educational process," 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2015, pp. 833-835.
[18] Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, and Chin- Chen Chang, “Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography,” Mobile Information Systems,vol. 2017, Article ID 4356038, 12 pages, 2017.
[19] Yang, Ching-Nung & Liao, Jung-Kuo & Wu, Fu-Heng & Yamaguchi, Yasushi. (2016). “Developing Visual Cryptography for Authentication on Smartphones”. 189-200. 10.1007/978-3-319-44350-8_19.
[20] Sangeeta Singh. May 2016. “QR Code Analysis” International Journal of Advanced Research in Computer Science and Software Engineering,Volume 6, Issue 5, ISSN: 2277 128.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY