Survey on Security Related to Visual Cryptography

V Gokula Krishnan[1], P Matan[2], R Ravichandran[3], C Varun Raman[4]
[1]*Associate Professor, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, Tamil Nadu, India*
[2, 3, 4]*UG Scholars, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, Tamil Nadu, India*

***Abstract*- The chance of the question paper getting leaked is increasing day by day and a solution is proposed to solve this problem. Elliptic Curve Cryptography (ECC) along with QR code will be a solution to this problem. QR code (Quick Response) is the trademark for a type of matrix (two dimensional) barcode. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary and kanji) to store data efficiently. Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. ECC technique involves conversion of text to cipher text. The cipher text is then converted to a QR Code. During decryption, the QR code is scanned and the content is decrypted. Only the application can read the original data shared in QR code since the data is encrypted with ECC with the integrity being maintained. An additional feature of linking the student's answer sheet with hall ticket and question paper is also added to avoid paper frauds and making re-evaluation a simpler task. Once the evaluation is done, the examiner can then scan the code and enter the mark in the student database which is maintained by the university.**

Index Terms- QR Code, ECC, RSA, DES, Encryption, Decryption.

INTRODUCTION

In this age of the digital era, with the progress of technology and continuous growth in digital data, there is an important need of optimization of data and information presently in the digital world. The authenticity of data is the trickiest issue in management of data in the internet database. In order to achieve this, we use cryptography.

Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. Cryptography allows people to keep confidence in the electronic world. People can do their business on electric channel without worrying of deceit and deception. Confidentiality, data integrity, authentication, and non-repudiation are central to cryptography. Modern cryptography exists in almost every discipline like mathematics, computer science and electrical engineering. Cryptography involves two methods called encryption and decryption. Encryption changes the plain text to cipher text using encryption algorithms such that no one other than the sender can make sense out of it using a key generated by the algorithm during the encryption process. Decryption is the reverse of encryption that is done on the receiving end. But in order to do it the receiver must have the knowledge of key otherwise he will not be able to make sense out of the received encrypted message.

In this, we mainly consider the problem of exam papers getting leaked. Keeping this problem in mind, we have introduced a new digital documentation system using QR codes. QR Code is a type of 2 dimensional matrix barcode, which is more popular than 1-D barcodes because of its large capacity of digital data and it can be readable in any mobile devices. By combining Elliptical Curve Cryptography with QR code, we can achieve a new level of reliable communication.

LITERATURE SURVEY

Sl. No	Title	Author Name	Journal	Advantages	Disadvantages
1	Probabilistic visual cryptography	S. Cimato, R. De Prisco, A.	*Comput. J.*, vol. 49, no. 1, pp. 97_107,	One-to-one correspondence between probabilistic schemes with	The probabilistic model of Yang considers visual cryptography

	schemes	De Santis	Jan. 2006.	no pixel expansion and deterministic schemes; such one-to one mapping trades the probabilistic nature of the scheme with the contrast of the deterministic scheme is shown.	schemes without pixel expansion; in such schemes the reconstruction of the secret pixel is probabilistic.
2	Halftone Visual Cryptography Via Error Diffusion	Z. Wang, G. R. Arce, G. Di Crescenzo	*IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383_396, Sep. 2009.	The pixels that carry the secret information are preset before a halftone share is generated from a gray scale image.	There is a trade-off between the share image quality and the contrast loss of the decoded image.
3	Perfect contrast XOR-based visual cryptography schemes via linear algebra	G. Shen, F. Liu, Z. Fu, B. Yu	*Des. Codes Cryptogr.*, vol. 85, no. 1, pp. 15_37, Oct. 2017.	Flexible sharing strategy, perfect visual quality, the sufficient and necessary conditions for the existence of a perfect XVCS.	Each participant has to carry multiple shares and is required to know at the time of revealing the secret for which access structures he is going to submit which of his shares.
4	Minimizing pixel expansion in visual cryptographic scheme for general access structures	S. J. Shyu, M. C. Chen	*IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 9, pp. 1557_1561, Sep. 2015.	Can be applied to construct the basis matrices with the minimum pixel for a GVCS. The optimal pixel expansion of a GVCS can be acquired.	The counting (or generation) of all non-reducible (strong) access structures for a general n is still an open problem.
5	On (k, n) Visual Cryptography Scheme	S. Arumugam, R. Lakshmanan, Atulya K. Nagar	*Des., Codes Cryptogr.*, vol. 71, no. 1, pp. 153_162, Apr. 2014.	The pixel expansion for *(k, n)*∗-VCS constructed by using the method proposed in this paper is much less than the pixel expansion of the corresponding VCS obtained by CA-method.	The relative contrast and the pixel expansion cannot be optimized simultaneously. Optimality with respect to contrast and optimality with respect to pixel expansion cannot be achieved by the same scheme.
6	Property Analysis of XOR-Based Visual Cryptography	Ching-Nung Yang, and Dao-Shun Wang	*IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 2,pp. 189_197, Feb. 2014.	It provides high contrast and good resolution for an image.	This method only applicable for the black and white images.
7	Visual Cryptography for General Access Structures	Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis and Douglas R. Stinson	*Inf. Comput.*, vol. 129, no. 2, pp. 86_106, Sep. 1996.	The participants in a qualified set X will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation.	To construct the visual cryptography scheme it needs two methods.
8	Adaptive halftoned visual cryptography with improved Quality and security	Srividhya Sridhar, R. Sathishkumar and Gnanou Florence Sudha	*Multimedia Tools Appl.*, vol. 76, no. 1, pp. 815_834, Jan. 2017.	This scheme provides a more efficient way to hide natural images in different shares.	Sometimes the shades cannot be printed out accurately.
9	Extended color visual cryptography for black and white secret image	Ching-NungYang, Li-Zhe Sun and Song-Ruei Cai	*Theor. Comput. Sci.*, vol. 609, pp. 143_161, Sep. 2016.	Has the same pixel expansion and contrast when compared with (k, n)-VCS. Meanwhile, our scheme provides the extended capability.	Construction of the non-perfect black (k, n)-CBW-VCS and (k, n)-CBW-EVCS deserves further studying.
10	General construction for XOR-based visual cryptography and its extended capability	Hao Hu, Gang Shen, Zhengxin Fu, Bin Yu and Jingjing Wang	*Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13883_13911, Jan. 2016.	Introduces a general construction of VCSXOR for strong access structures, which achieves merits such as various sharing strategies, perfect reconstruction and better visual quality.	This algorithm works for only the black and white images.
11	Progressive Visual Cryptography with Unexpanded Shares	Young-Chang Hou and Zen-Yu Quan	*IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1760_1764, Nov. 2012.	The original secret can be visually obtained only when a subset of at least *k* shares are available and are well stacked together.	The increase of the numbers of shares being stacked, the contrast between white and black regions will be increased, hence reveals the content of the secret image progressively.
12	Embedded Extended Visual Cryptography Schemes	Feng Liu and Chuankun Wu, Senior Member, IEEE	*IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307_322, Jul. 2011.	Any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image	The black ratio is high, the darkening process will decrease the visual quality of the covering shares.

CONCLUSION

In this paper, we are able to bring a solution to the question paper getting leaked. We are able to encrypt the question paper using Elliptical Curve Cryptography and make it into a QR code. There is no data loss at all and complete integrity of the file is maintained throughout the process. Additionally, we are able to access the question paper only 2 hours in prior to the exam and not before that, thereby preventing any chances of leaking. We are also able to track the student's attendance for the exam and have made it possible for the evaluator to enter the marks a very easy process.

REFERENCES

[1] M. Naor and A. Shamir, ''Visual cryptography,'' in Advances I Cryptology - EUROCRYPT (Lecture Notes in Computer Science), vol. 950, A. De Santis Eds. Berlin, Germany: Springer-Verlag,May 1995,pp. 1–12.

[2] C.-N. Yang and D.-S. Wang, ''Property analysis of XOR-based visual cryptography,'' IEEE Trans. Circuits Syst. Video Technol., vol. 24, no. 2, pp. 189–197, Feb. 2014.

[3] G. Shen, F. Liu, Z. Fu, and B. Yu, ''Perfect contrast XOR-based visual cryptography schemes via linear algebra,'' Des. Codes Cryptogr., vol. 85, no. 1, pp. 15–37, Oct. 2017.

[4] S. J. Shyu and M. C. Chen, ''Minimizing pixel expansion in visual crypto- graphic scheme for general access structures,'' IEEE Trans. Circuits Syst. Video Technol., vol. 25, no. 9, pp. 1557–1561, Sep. 2015.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, ''Visual cryptography for general access structures,'' Inf. Comput., vol. 129, no. 2,pp. 86–106, Sep. 1996.

[6] S. Arumugam, R. Lakshmanan, and A. K. Nagar, ''On (k, n)∗-visual cryptography scheme,'' Des., Codes Cryptogr., vol. 71, no. 1, pp. 53–162,Apr. 2014.

[7] S. Sridhar, R. Sathishkumar, and G. F. Sudha, ''Adaptive halftoned visual cryptography with improved quality and security,'' Multimedia Tools Appl., vol. 76, no. 1, pp. 815–834, Jan. 2017.

[8] C.-N. Yang, L.-Z. Sun, and S.-R. Cai, ''Extended color visual cryptography for black and white secret image,'' Theor. Computer. Sci., vol. 609,pp. 143–161, Sep. 2016.

[9] H. Hu, G. Shen, Z. Fu, B. Yu, and J. Wang, ''General construction for XOR-based visual cryptography and its extended capability,'' Multimedia Tools Appl., vol. 75, no. 21, pp. 13883–13911, Jan. 2016.

[10] Y.-C. Chen, ``Fully incrementing visual cryptography from a succinct non monotonic structure," IEEE Trans. Inf. Forensics Security, vol. 12, no. 5, pp. 1082_1091, May 2017.

[11] Y.-C. Hou and Z.-Y. Quan, ``Progressive visual cryptography with unexpanded shares," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1760_1764, Nov. 2012.

[12] F. Liu and C. Wu, ``Embedded extended visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307_322, Jul. 2011.

[13] D. Wang, F. Yi, and X. Li, ``On general construction for extended visual cryptography schemes," Pattern Recognit., vol. 42, no. 11, pp. 3071_3082, Nov. 2009.

[14] I. Kang, G. R. Arce, and H.-K. Lee, ``Color extended visual cryptography using error diffusion," IEEE Trans. Image Process., vol. 20, no. 1, pp. 132_145, Jan. 2011.

[15] X. Yan, S. Wang, X. Niu, and C.-N. Yang, ``Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality," Digit. Signal Process., vol. 38, pp. 53_65, Mar. 2015.