International Journal for Modern Trends in Science and Technology
Volume 9, Issue 08, pages 131-137.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol9issue08.html
DOI: https://doi.org/10.46501/IJMTST0908020

Visual Cryptography: A Brief Review

Venkata Narayana Reddy[1], Patan Arifoon[2]

[1]Academic consultant, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India.
[2]Lecturer, Department of Computer Science and Applications, Nagarjuna Women's Degree and PG college, Kadapa, India

To Cite this Article
Venkata Narayana Reddy and Patan Arifoon, Visual Cryptography: A Brief Review, *International Journal for Modern Trends in Science and Technology*, 2023, 9(08), pages. 131-137. https://doi.org/10.46501/IJMTST0908020

Article Info
Received: 18 July 2023; Accepted: 26 August 2023; Published: 29 August 2023.

ABSTRACT

Cryptography has different procedures that are helped to encrypt correspondence and to ensure a secured and controlled data exchange between the sender and recipient. In Elliptic Curve Cryptography (ECC), the proposed algorithm would play a crucial role in tackling all the problems related to the key exchange. This paper also shows an ECC analysis covering the ECC algorithm method, the basic ECC algorithm protocols, the varied ECC development and the ECC utilization. This article also represents different graphical presentations of the EC visual cryptographic mechanism over the endless and endless areas.

KEY WORDS: Elliptic Curve Cryptography, Visual Crypto Grapy, Random grid based visual cryptography, Key generation.

I. INTRODUCTION

Nowadays, one of the primary issues of every contact is security. As a result, cryptography is used to encrypt correspondence between senders and receivers. Cryptography has been used for several centuries [1]and is characterized as a process, procedure, or multiple formulas that protect data or networks to achieve Integrity, Authentication, Confidentiality, Access Control, Non-repudiation and Availability by sending the information to unreadable format[2][3][4]. Since the invention of cryptography with the public key in 1976 by Martin Hellman and Whit Diffie, the relevance of cryptography has been widely recognized, and the discrete logarithm problem has been thoroughly researched[5][6]. Cryptography is divided into three major categories: Secret Key, Public Key, and Hash Functions. One key is used for both encryption and decryption in symmetric cryptography, commonly termed private key cryptography. However, in asymmetric cryptography or shared key cryptography, two keys are used: a public key to cypher or decrypt the transmitted message and a private key used by the key holder to decrypt the data[7][8]. The term "public key cryptography" comes from the fact that the coding of the message was made freely accessible [9][10]. ECC is a form of public-key cryptography that is also known as asymmetric-key cryptography [11][12]. This paper would include an overview of ECC.

II. OVERVIEW OF ECC

ECC is a public or asymmetric key cryptography that was introduced in 1985 by both Victor Miller and Neil Koblitz and is strictly mathematical in nature [13]. The distinguishing feature of ECC is that it provides its users with a small key size and a challenging expanding time threat to the intruder to break the device or contact[14]. Since 160 bits of ECC equals 1024 bits of RSA at a ratio of 1:7, ECC offers similar protection as RSA but with a smaller key size. As a result, ECC has a small key size, strong security, and quicker cryptographic procedures since it uses lightweight chips and software [15]. The cryptosystem in ECC needs three algorithms: Key

generation, encryption algorithm, and decryption algorithm, which are all, tested using the regional specifications of the Elliptic Curve (EC)[16]. In ECC, two keys must be produced: The public key, which is passed down by the data owner to encrypt the data and transform it to ciphertext, and the private key, which is held by the owner and is used to decrypt the ciphertext and translate it to a readable form[15]. The EC Discrete Logarithm problem over a finite field or integer factorization is the sole foundation of ECC[17]. The ECC is based on the general equation (1)

$$y^2 = x^3 + ax + b \qquad (1)$$

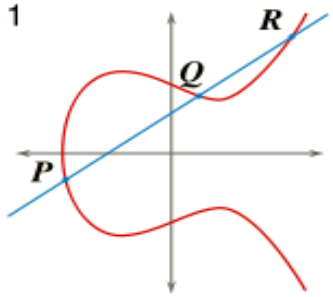

Fig. 1: EC illustrates the operation P+Q=R

III. ECC over finite field mathematics

With the use of coordinate points of EC, a cryptographic process on EC over a finite field is done. The given formula $y^2 = x^3 + ax + b$ mod p illustrates the ECover finite field equation [18]. Separate rubrics are located for the procedure with the points which are point adding, subtraction, doubling and point multiplication[19].

A. EC point adding

The two points $P(x_1, y_1)$ and $P(x_2, y_2)$ are different and to achieve the computations, the two points are added to generate the point $R(x_3, y_3)$. Fig. 2 shows EC point adding graphical representation

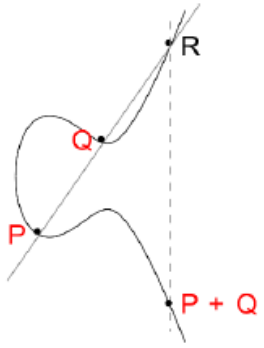

Fig. 2: EC Point additions [18]

B. EC point subtraction

We conduct point subtraction by finding the reflect coordinate of the subtracted point and adding the created coordinate point, and then subtracting this number from the first one [10].

C. EC point Doubling

To double the point means to connect two identical points, each of which has the same coordinate value. Figure 3 illustrates the effect of doubling the electric current point.

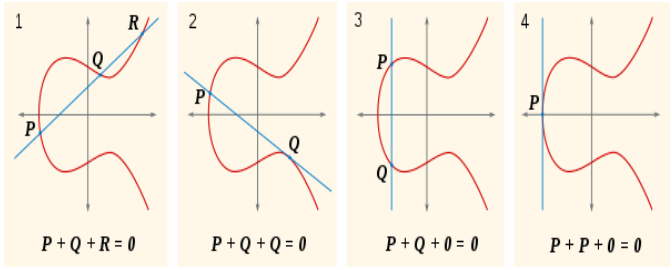

Fig.3: Various operations on EC

D. EC point multiplication

The point multiplication equation says that the result of adding the same point (say P) to itself n times is equal to nP= P+P + P + P + P…P. to stress importance expand, go on

E. Point at infinity

The intersection of the points is at the infinity is represented as 0 and that happened when the points of x_1 is equal to x_2 and y_1 is equal to y_2 so it equal to 0 or x_1 is equal to x_2 and y_1 is equal to $-y_2$.

IV. Process of ECC Algorithm

Some procedures need to be taken to use the ECC algorithm

Step 1: The general formula: $y^2 = x^3 + ax + b$ where a and b are the curve specifications

Step 2: Two prime numbers are selected

Step 3: The next step is to find adding and doubling points on the curve.

Step 4: You have to choose a generating point other than the points that were already used to increase the sequence duration.

Step 5: The fifth step is to use a number that is smaller than the point from which the numbers are produced and use it as a private number for each person.

Step 6: To complete the process, the public key is created by multiplying the produced number with the secret number.

To further illustrate this method, the following statement would address the creation of keys, the process of computing a hidden key, and the process of exchanging keys. One factor, in particular, the elliptic curve element (or equation) with Eq(a,b) (where q is an integer or a prime number of form 2m and G is the Generator), has two features: First, the q parameter (which is an integer or a prime number of form 2m) must be specified. Second, the order of the G Generator must be high (that is, the order of the G Generator must be greater than 2m).

F. Generation of Key

The first step to start the encryption is generating keys by selecting numbers and multiplies it with the generator[20]. It has another two steps such as alias key generation and bob key generation. In alias key generation, a secret number is selected which is less than the large number and the public key is generated. Whereas in bob key generation process, the secreted key is selected which isles than the large size key and the public key is generated.

G. In this step, from the above data, both keys are calculated

H. Encryption of the message by Alice using public key of Bob

I. Decryption of the received cipher text by Bob using his own Private key

J. Key Exchange

V. Basic protocols of ECC algorithm

With respect to the digital signature and key exchange, there are several general ECC algorithms that can be employed. The elliptic curve digital signature algorithm (ECDSA) (ECDSA). For the most part, DS is added to authenticate the devices, or the message is transmitted from the computer such that the message is sent with sign signature in order to guarantee that the message is not tampered with anybody[21]. ECDSA is part of the ANSI and IEEE standards committees. There are differences in DSA; nevertheless, it runs on EC units. In order to transmit a message using the electronic medium, both the sender and receiver of the message must have agreed on the EC domain parameters. One simple, basic, definition of this will be if the parties are Alice and Bob, where Alice is the sender and Bob is the receiver. Her dA (privately produced random number) and QA (publicly generated random number) represent a key pair in which QA = G. G is the randomly generated point on elliptic curve domain parameters. (Increasingly) increasing. Elliptic Curve Diffie Hellman Key Exchange and Elliptic Curve Diffie Hellman Key Exchange (ECDH) The arrangement to enable the communication party to establish a common secret key which can be included in the private key algorithm serves as a way for them to make the communication possible. Before the actual process of exchanging information and computing the shared secret key begins, the parties are required to disclose some aspects of their relationship. They do this by utilizing their own private key and the public information, which results in their being able to calculate the shared secret key. Other than when dealing with a faction, it would be impossible for any external party to determine the mutual secret key from the public knowledge available. The protocol uses EC domain parameters to construct a mutual secret key between Alice and Bob. No party has to worry about conflicting parameters for EC names. In addition to both a secret and public key, Alice and Bob both have a key consisting of a private key d (dA, dB) and a public key QA= G.dA and QB= G.dB, respectively. A and B are therefore, the private and public keys of Alice are (D, Q) and the private and public keys of Bob are D and Q (dB, QB). Alice then calculates E=xE + yE = dA. A quarterback where x and y are the domain parameters of EC. On the other side, Bob figured out that F=(xF,yF)=dB.QA. As a result, dAQB = dAdBG = dBdAG = dBQA. The following statements are both equivalent: E is identical to F, and xE = xF. Because of this, the mutual hidden key is xE. Taking into account the math used above, the result of the equations is that it is not feasible to uncover the private keys of Alice and Bob (dA and dB) using the public keys E and F. Third parties do not have access to the shared private key, so it is difficult to procure it.

VI. ECC Implementation

These portable gadgets have come to play a significant role in the modern era. Even, these machines are equipped with minimal memory, so in order to accommodate the need for protection, additional memory is needed. This is what makes a problem when the security is required as specified. Due to the low-key scale of ECC, which uses scalar multiplication, point

addition, and point doubling, ECC is generally regarded as the best possible choice for smaller memory devices, such as smart phones, palmtop, and smartcards utilizing scalar multiplication, point addition, and point doubling[22]. For eg, in radio frequency identification (RFID), ECC was implemented and demonstrated that it offers legitimate protection for data combination and memory access that's marked with a radio frequency identification chip. Additionally, since it reduces the necessary storage for the key and the backend device, by does so by keeping the private key only, this is a good idea. As a result, the commutation of the tag is reduced [23]. In addition. Cryptography with the elliptic curve's main advantages is appealing for the implementation in handheld or wireless settings.

VII. ECC applications

In real world, ECC is applied in different areas and technologies. Below are some of them.

A. Bitcoin

In the crypto currency system of Bitcoin, the flow of payment does not happen in the form of a transaction via a financial institution, but directly amongst peers. In Bitcoin, the decentralized block chain is a continuously-collected grouping of regular transaction histories. For any block in this group, the prior block's hash is hashed and added to the end of the block's previous hash, such that the chain begins from the origin block[24]. In the case of Bitcoin, a user account serves as ECDSA private key, which enables the verification of who has acquired control of the bitcoins between senders and receivers by first linking a DS with the private key of the sender of the previous hash activity and the public key information of the receiver[25]. As we can see that the sender's public key from the previous transaction has been used in authentication, the same procedure can be implemented here.

B. Secure Shell (SSH)

Though there are several areas in which ECC can be implemented, SSH utilizes it in certain locations. By default, clients and servers are configured with host keys that make it possible for them to prove to each other that they are who they say they are. When the client and the server come to an agreement on a session key, the server sends it to the client such that the client checks to see if the fingerprint corresponds to the saved value [26]. Once the server has created a copy of the exchange key and ECDSA may be used as the key, the server then conducts a self-authenticity by signing its own exchange key [27].

C. Austrian e-ID

Though there are many options for granting users entry to the network, the most commonly used approach is a physical smart card that is used to authenticate users. Cryptographic computations are carried out using smart cards that carry cryptographic hardware modules. Each of these hardware modules holds a private key used for encryption and signatures. In this context, the phrase “less computational complexity of ECC” means that ECC is more suited for use in applications that require security, and since the security uses are of lower computation complexity, ECC is often implemented in such applications. For digital signatures to be accepted as legally binding, ECDSA public key cab be used[28].

D. Transport Layer Security (TLS)

The EC may be seen in a variety of locations in the procedure. ECDH is a fundamental building block of all encryption cyphers that use the RFC suite. The certificates that encrypt data using TLS contain a cryptographic key that is used by the server to identify itself and the usage of ECDSA is this public key[29]. TLS used the use of Elliptic Curve Cryptography (ECC) in the client and server hello communications, as well as another collection of cipher suites and. The suites advocate that elections should be held to decide upon the preferred exchange, encryption, and authentication algorithms for message and identity verification[22]. Instead of submitting the whole options list of curves and cypher suites that the server is using, a smaller subset of those options is sent to the client, and the server will choose only those responding with a single cypher suite from the list that the client provided. If the link is terminated for refusing to use any of the cyphers or curves in the list, it was not handled by this feature[30]. To help the suite access the ECC functionality, only one curve sort, and one with a key or signature, is available in the api. The problem with trying to find out whether the server accepts various TLS curves is that a client must make several TLS connections in order to provide a variable number of curves and therefore discover what order of choice the server values these various curves [31].

VIII. Visual cryptography (VC)

Traditional cryptography techniques are computationally intensive, both in the encryption and decryption processes. The primary issue in the field of cryptography is the secure transmission of multimedia data over the internet [32][33]. Visual cryptography (VC) is a sophisticated technique that blends the cryptographic concepts of perfect ciphers and secret sharing with those of raster graphics. A binary image can be partitioned into shares, each of which can be stacked to approximate the original image. A secret sharing scheme enables the distribution of a secret among n parties in such a way that the secret can be reconstructed only by predefined allowed sets [34][35]. Visual cryptography allows for the visual reconstruction of the password by superimposing shares[36].

Visual cryptography (VC) is another method for securely encrypting secret image (SI) data. In VC, an original image is encrypted and divided into multiple images known as shares. The original image is referred to as SI, and it is encrypted using various VC techniques; shares are encrypted versions of SI[37]. These shares are allocated to various participants. The SI cannot be determined based on a single share. The original picture is recovered when these shares are stacked together. VC is a form for binary, or white and black, SI sharing. When these shares are stacked together, the human visual system can quickly decrypt them [38][39]. (HVS). As a result, no computation is required and cryptographic knowledge is required. The problem of pixel expansion plagues traditional visual cryptography schemes (VCS) [40]. SI transforms this image into larger shares, i.e., m times the original image's size. Visual Secret Sharing (VSS) is a technique for safely encrypting a SI and distributing it to shares. The advantages of these schemes are that HVS can easily decode SIs, and no cryptographic computations or knowledge of cryptography are needed[41]. The concept of image sharing is similar to the concept of general secret sharing. In (x, y) image sharing, the hidden image is divided into y pieces (referred to as shares), and decryption is impossible until at least x pieces are collected and superimposed. Fig. 1 illustrates the various forms of sharing patterns [42].

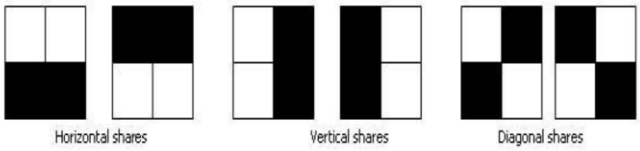

Fig 4: The numerous pixel patterns that are used to create VC shares

Color Visual cryptography

Visual cryptography techniques applied to color images are critical because they allow the use of natural color images to protect certain types of information. Due to the existence of a color picture, this further reduces the risk of alerting anyone to the fact that information is concealed within it. Additionally, it should allow high-quality sharing of these color images [43]. Fig.5 illustrates a simple (2, 2) color visual cryptography scheme. Two distinct color shares are generated at random. By OR'ing each of them, the secret can be retrieved. Although the contrast difference is quite obvious, the consistency of the recovered secrets is quite remarkable [44][45].

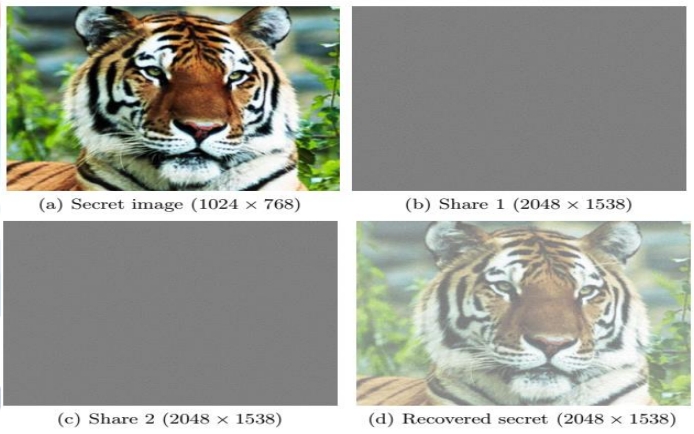

Fig 5: The outcome of a two-color (2, 2) VC scheme

Random grid based visual cryptography

Kafri and Keren introduced the definition of random grid (RG) in 1987. RG is transparency that consists of a two-dimensional array of pixels [46][47]. We may obtain each pixel that is either opaque or fully transparent in a random manner using the coin flip technique. As a result, there is no connection between the values of the array's pixels. The opaque pixels block the light, while the transparent pixels allow it to pass through. Probabilistically, the number of opaque pixels equals the number of visible pixels in an RG[48][49]. Thus, a random grid's average light transmission is ½ [50].VC's approach enables global decoding rather than point-wise

decoding. This technique is based on the generalized moiré effect obtained by the use of RG. The information-containment areas of the two RG are associated. Owing to the disparity in light propagation, the correlated areas will be resolved after stacking these two grids. The decryption operation is identical to that specified in traditional VCS[51][52].

IX. Conclusions

Although it is extremely easy to distribute and access images through the internet nowadays, there is a security aspect to consider when transmitting data. Image encryption is one way of preventing unauthorized access to files. As a result, this field of protection is a hot topic for researchers. ECC is a widely employed asymmetric or shared key cryptography with three major algorithms: key creation, encryption, and decryption. Because of its limited scale and complex algorithm, it raises the standard of confidentiality, making it almost impossible for third parties or attackers to break the connection.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

[1] R. Bhanot and R. Hans, "A Review and Comparative Analysis of Various Encryption Algorithms," Int. J. Secur. its Appl., vol. 9, pp. 289–306, 2015.

[2] A. K. Singh, "A Review of Elliptic Curve based Signcryption Schemes," Int. J. Comput. Appl., vol. 102, no. 6, p. 8887, 2014.

[3] D. Mahto and D. K. Yadav, "RSA and ECC,A Comparative Analysis.pdf," Int. J. Appl. Eng. Res., vol. 12, no. 19, pp. 9053–9061, 2017.

[4] R. Shaik, N. K. Gudapati, N. K. Balijepalli, and H. R. Medida, "A Survey on Applications of Internet of Things," Int. J. Civ. Eng. Technol., vol. 8, no. 12, pp. 558–571, 2017, doi: 10.1109/IS48319.2020.9200185.

[5] K. Vasundhara, Y. V S Sai Pragathi, and Y. Sai Krishna Vaideek, "A Comparative Study of RSA and ECC," Int. J. Eng. Res. Appl. www.ijera.com, vol. 8, no. 1, pp. 49–52, 2018, doi: 10.9790/9622-0801014952.

[6] S. R, "Dual Server based Security Protocol in MANET using Elliptic Curve Cryptography: A Cluster Head Selection Scenario," Int. J. Adv. Trends Comput. Sci. Eng., vol. 6, pp. 1621–1629, 2019, doi: 10.30534/ijatcse/2019/87842019.

[7] C. Pradeep, M. Rao, and B. Vikas, "Quantum Cryptography Protocols for Internet of Everything: General View," 2021, pp. 211–218.

[8] A. Oad, H. Yadav, and A. Jain, "A Review : Image Encryption Techniques and its Terminologies," Int. J. Eng. Adv. Technol., vol. 3, no. 4, pp. 373–376, 2014.

[9] M. Parvez, "Network Security using Notable Cryptographic Algorithm for IoT Data," Int. J. Emerg. Trends Eng. Res., vol. 8, pp. 2169–2172, 2020, doi: 10.30534/ijeter/2020/111852020.

[10] M. Benssalah, Y. Rhaskali, and K. Drouiche, "An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography," Multimed. Tools Appl., vol. 80, no. 2, pp. 2081–2107, 2021, doi: 10.1007/s11042-020-09775-9.

[11] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," Signal Processing, vol. 155, pp. 391–402, 2019, doi: 10.1016/j.sigpro.2018.10.011.

[12] V. S. Miller, "Use of Elliptic Curves in Cryptography," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 218 LNCS, pp. 417–426, 1986, doi: 10.1007/3-540-39799-X_31.

[13] Sujith Narayan, "a Review on Elliptic Curve Cryptography," Int. J. Emerg. Technol. Innov. Eng., vol. 4, no. 12, pp. 132–138, 2018.

[14] M. Bafandehkar, S. M. Yasin, R. Mahmod, and Z. M. Hanapi, "Comparison of ECC and RSA Algorithm in Resource Constrained Devices," in 2013 International Conference on IT Convergence and Security (ICITCS), 2013, pp. 1–3, doi: 10.1109/ICITCS.2013.6717816.

[15] D. P. Rajesh, D. M. Alam, D. M. Tahernezhadi, T. Ravi Kumar, and V. P. Rajesh, "Secure communication across the internet by encrypting the data using cryptography and image steganography," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 10, pp. 454–458, 2020, doi: 10.14569/IJACSA.2020.0111057.

[16] M. Arif, A. H. M. A. Habib, I. Rufat, and S. Azer, "Study and Implementation of Elliptic Curve Encryption Algorithm for Azerbaijan E-ID Card," 2015.

[17] B. Murali Krishna, H. Khan, and G. L. Madhumati, "Reconfigurable pseudo biotic key encryption mechanism for cryptography applications," Int. J. Eng. Technol., vol. 7, no. 1.5 Special Issue 5, pp. 62–70, 2018, doi: 10.14419/ijet.v7i1.5.9124.

[18] L. D. Singh and K. M. Singh, "Image Encryption using Elliptic Curve Cryptography," Procedia Comput. Sci., vol. 54, no. April, pp. 472–481, 2015, doi: 10.1016/j.procs.2015.06.054.

[19] M. Al Saadi and B. Kumar, "A Review on Elliptic Curve Crytography," Int. J. Futur. Gener. Commun. Netw., vol. 13, no. 3, pp. 1597–1601, 2020.

[20] S. R, "Elliptic Curve Cryptography Based Security Protocol of MANET under Dynamic Cluster Head Selection Environment," Int. J. Emerg. Trends Eng. Res., vol. 8, pp. 447–454, 2020, doi: 10.30534/ijeter/2020/32822020.

[21] V. Kapoor, V. S. Abraham, and R. Singh, "Elliptic Curve Cryptography," ACM Ubiquity, vol. 9, no. 20, pp. 1–8, 2008.

[22] L. D. Singh and K. M. Singh, "Image Encryption using Elliptic Curve Cryptography," Procedia Comput. Sci., vol. 54, pp. 472–481, 2015, doi: 10.1016/j.procs.2015.06.054.

[23] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8437, pp. 157–175, 2014, doi: 10.1007/978-3-662-45472-5_11.

[24] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," J. Supercomput., vol. 75, no. 10, pp. 6663–6682, 2019, doi: 10.1007/s11227-019-02878-7.

[25] E. Babu, C. Raju, and M. Prasad, "Inspired pseudo biotic DNA based cryptographic mechanism against adaptive cryptographic attacks," vol. 18, pp. 291–303, 2016.

[26] M. Dusi, F. Gringoli, and L. Salgarelli, "A model for the study of privacy issues in secure shell connections," Proc. - 4th Int. Symp. Inf. Assur. Secur. IAS 2008, pp. 311–317, 2008, doi: 10.1109/IAS.2008.46.

[27] M. S. N. G. K. Mounika, A. Yadav, S. L. Anand, and P. Satyannarayana, "Upgrade of GSM security using elliptic curve cryptography algorithm," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 7, pp. 487–491, 2019.

[28] V. B. Kute, P. R. Paradhi, and G. R. Bamnote, "A software comparison of RSA and ECC," Int. J. Comput. Sci. Appl., vol. 2, no. 1,

pp. 61–65, 2009, [Online]. Available: http://www.researchpublications.org/IJCSA/issue4/2009-IJCSA-02-01-15.pdf.
[29] M. Khalid, K. Arora, and N. Pal, "A Crypto-Steganography: A Survey," Int. J. Adv. Comput. Sci. Appl., vol. 5, no. 7, pp. 149–155, 2014, doi: 10.14569/ijacsa.2014.050722.
[30] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," Multidimens. Syst. Signal Process., vol. 32, no. 1, pp. 281–301, 2021, doi: 10.1007/s11045-020-00739-8.
[31] B. Jyoshna and K. Subramanyam, "Time conserving secured cloud data storage solution based on keccak and elliptic curve cryptography," Int. J. Adv. Res. Eng. Technol., vol. 10, no. 5, pp. 154–165, 2019, doi: 10.34218/IJARET.10.5.2019.016.
[32] A. M. Qadir and N. Varol, "A review paper on cryptography," 7th Int. Symp. Digit. Forensics Secur. ISDFS 2019, no. June, pp. 1–6, 2019, doi: 10.1109/ISDFS.2019.8757514.
[33] S. Shivani and S. Agarwal, "VPVC: verifiable progressive visual cryptography," Pattern Anal. Appl., vol. 21, no. 1, pp. 139–166, 2018, doi: 10.1007/s10044-016-0571-x.
[34] J. Wohlwend, "Elliptic Curve Cryptography: Pre and Post Quantum," pp. 1–17.
[35] S. Shivani, "Multi secret sharing with unexpanded meaningful shares," Multimed. Tools Appl., vol. 77, no. 5, pp. 6287–6310, 2018, doi: 10.1007/s11042-017-4536-x.
[36] M. Naor and A. Shamir, "Visual Cryptography Scheme," Proc. Adv. Cryptol., vol. 9, no. 12, pp. 1–6, 1994.
[37] K.Shankar and P.Eswaran, "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm," Adv. Intell. Syst. Comput., vol. 394, pp. 1105–1111, 2016, doi: 10.1007/978-81-322-2656-7.
[38] R. G. Sharma, P. Dimri, and H. Garg, "Visual cryptographic techniques for secret image sharing: a review," Inf. Secur. J., vol. 27, no. 5–6, pp. 241–259, 2018, doi: 10.1080/19393555.2019.1567872.
[39] S. Shivani and S. Agarwal, "VPVC: verifiable progressive visual cryptography," Pattern Anal. Appl., vol. 21, no. 1, pp. 139–166, 2018, doi: 10.1007/s10044-016-0571-x.
[40] J. Tripathi, A. Saini, Kishan, Nikhil, and Shazad, "Enhanced Visual Cryptography: An Augmented Model for Image Security," Procedia Comput. Sci., vol. 167, no. 2019, pp. 323–333, 2020, doi: 10.1016/j.procs.2020.03.232.
[41] K. Shankar and P. Eswaran, "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography," Procedia Comput. Sci., vol. 70, pp. 462–468, 2015, doi: 10.1016/j.procs.2015.10.080.
[42] J. Weir and W. Q. Yan, "A comprehensive study of visual cryptography," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6010 LNCS, no. Vc, pp. 70–105, 2010, doi: 10.1007/978-3-642-14298-7_5.
[43] N. K. Prakash and S. G. Govindaraju, "Visual Cryptography Scheme for Color Images Using Half Toning Via Direct Binary Search with Adaptive Search and Swap," Int. J. Comput. Electr. Eng., vol. 3, no. 6, pp. 900–904, 2011, doi: 10.7763/ijcee.2011.v3.440.
[44] D. Wang, L. Dong, and X. Li, "Towards Shift Tolerant Visual Secret Sharing Schemes," IEEE Trans. Inf. FORENSICS Secur., vol. 6, no. 2, pp. 323–337, 2011.
[45] D. Ou and W. Sun, "High payload image steganography with minimum distortion based on absolute moment block truncation coding," Multimed. Tools Appl., vol. 74, no. 21, pp. 9117–9139, 2015, doi: 10.1007/s11042-014-2059-2.
[46] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett., vol. 12, no. 6, pp. 377–379, Jun. 1987, doi: 10.1364/OL.12.000377.
[47] X. Yan, X. Liu, and C.-N. Yang, "An enhanced threshold visual secret sharing based on random grids," J. Real-Time Image Process., vol. 14, no. 1, pp. 61–73, 2018, doi: 10.1007/s11554-015-0540-4.
[48] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography," Signal Processing, vol. 125, pp. 187–202, 2016, doi: 10.1016/j.sigpro.2016.01.017.
[49] D.-S. Tsai, G. Horng, T.-H. Chen, and Y.-T. Huang, "A novel secret image sharing scheme for true-color images with size constraint," Inf. Sci. (Ny)., vol. 179, no. 19, pp. 3247–3254, 2009, doi: https://doi.org/10.1016/j.ins.2009.05.020.
[50] S. J. Shyu, "Image encryption by random grids," Pattern Recognit., vol. 40, no. 3, pp. 1014–1031, 2007, doi: 10.1016/j.patcog.2006.02.025.
[51] X. Wu and W. Sun, "Improved tagged visual cryptography by random grids," Signal Processing, vol. 97, pp. 64–82, 2014, doi: https://doi.org/10.1016/j.sigpro.2013.10.023.
[52] Y.-S. Lee and T.-H. Chen, "Insight into collusion attacks in random-grid-based visual secret sharing," Signal Processing, vol. 92, no. 3, pp. 727–736, 2012, doi: https://doi.org/10.1016/j.sigpro.2011.09.015.