

A NEW MODIFIED GRAYSCALE IMAGE ENCRYPTION TECHNIQUE USING ELLIPTIC CURVE CRYPTOSYSTEM

ZIAD E. DAWAHDEH¹, MOHAMMED AMIN ALMAIAH^{2,3}, TAYSEER ALKHDOUR⁴,
ABDALWALI LUTFI^{5,6}, THEYAZN H. H. ALDHYANI⁷, AND QUSAY BSOUL⁸

¹ Computer Studies Department, Arab Open University, Amman, Jordan

² King Abdullah the II IT School, the University of Jordan, Amman 11942, Jordan

³ Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan

⁴ College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

⁵ College of Business, King Faisal University, Al-Ahsa, 31982, Saudi Arabia.

⁶ MEU Research Unit, Middle East University, Amman, Jordan

⁷ Applied College in Abqaiq, King Faisal University, Al-Ahsa 31982, Saudi Arabia

⁸ College of Information Technology, Applied Science Private University, Amman 11931, Jordan

Corresponding authors: talkhdour@kfu.edu.sa and m.almaiah@ju.edu.jo

ABSTRACT

Image encryption is one of the interested and important topics that recently spread as a result of the growing usage of the internet and other forms of communication in order to protect images from stealing and attacks. This work proposes a novel improvement to Menezes-Vanstone Elliptic Curve Cryptography to improve grayscale image encryption and decryption. The new modification in this paper reduces the encryption and decryption needed running time and speed up calculations. In the new method, no need for inverse and multiplication operations, only addition and subtraction are used, and this speeds up computations and reduces running time than other methods. Moreover, the modification makes the algorithm more secure and difficult for the attackers to attack it. Entropy, Unified Average Changing Intensity (UACI), and Peak Signal to Noise Ratio (PSNR) will be utilized to evaluate the grayscale image encryption efficiency. A comparison of the encrypted image and the original image will be performed to assess the performance of the suggested encryption approach.

Keywords: *Entropy, Unified Average Changing Intensity, Peak Signal to Noise Ratio, Elliptic Curve Cryptography, and Menezes-Vanstone Elliptic Curve Cryptosystem.*

1. INTRODUCTION

Image encryption is an important area of research and development, as the increasing use of digital images for communication and storage has made them more vulnerable to unauthorized access and tampering [1-3]. There are many different approaches to image encryption, ranging from simple techniques that use a single key to more complex methods that involve multiple keys or use advanced cryptographic algorithms. Cryptography is a set of mathematical techniques that can be used to secure the confidentiality, integrity, and authenticity of information, including images, as it is transmitted over a non-secure channel. Cryptography allows two parties

who do not necessarily trust each other to communicate securely, by using mathematical algorithms to encode (encrypt) and decode (decrypt) messages [4-8]. Cryptography can be used to secure the transmission of images over a non-secure channel by encrypting the images before they are transmitted and decrypting them upon receipt. This can help to protect the confidentiality of the images and prevent unauthorized access or tampering [9-12]. However, it is important to use strong cryptographic algorithms and keys to ensure the security of the transmitted images.

There are two main types of cryptography: symmetric key cryptography and public key

cryptography. In symmetric key cryptography, both parties use the same key to encrypt and decrypt messages. This can be efficient, but it requires that the key be shared securely between the parties, which can be challenging [13]. In public key cryptography, each party has a pair of keys: a public key and a private key. The public key is used to encrypt messages, while the private key is used to decrypt them. This allows parties to communicate securely without having to share a key beforehand. While, symmetric key cryptography, also known as secret key cryptography, is a type of cryptography in which the same key is used to both encrypt and decrypt messages. This type of cryptography is efficient and easy to implement, but it requires that the key be shared securely between the parties who are communicating [14-18]. In symmetric key cryptography, the sender and the receiver use the same key to encrypt and decrypt the message. The key is typically a string of bits that is used to transform the message in some way, such as by shifting the letters of the message by a certain number of places or by substituting one letter for another. There are several different algorithms that can be used for symmetric key cryptography, including block ciphers and stream ciphers [19-22]. Block ciphers operate on fixed-size blocks of data, while stream ciphers operate on a stream of data. Symmetric key cryptography is widely used for secure communication, including in applications such as email, file transfer, and online banking. However, it has some limitations, such as the need to securely share the key between the parties, which can be challenging in some situations [23].

ElGamal encryption scheme, which is a public key encryption system is based on the mathematical concept of an elliptic curve, which is a curve defined by an equation of the form $y^2 = x^3 + ax + b$. In the ElGamal scheme, the keys are derived from the points on an elliptic curve, and the encryption and decryption of messages is performed using mathematical operations on these points. Overall, the ElGamal scheme and its variants are considered secure methods of encryption, as they are based on the difficulty of finding discrete logarithms in a finite field. However, they can be computationally intensive, which can make them less practical for certain applications [24].

Menezes-Vanstone Elliptic Curve Cryptography (MVECC) is a variant of the ElGamal encryption

scheme, which is a public key encryption system that uses multiple keys and ciphers to encrypt and decrypt messages. It is based on the mathematical concept of an elliptic curve, and the keys are derived from points on the curve. In MVECC, a message is encrypted using multiple keys and ciphers, which makes it more difficult for an attacker to decrypt the message without the appropriate keys. MVECC involves breaking the message into two parts and encrypting each part with a different key [25-27]. This makes it more difficult for an attacker to decrypt the message, as they would need to find both keys in order to retrieve the original message. Overall, MVECC is considered to be a secure method of encryption, as it is based on the difficulty of finding discrete logarithms in a finite field. However, it can be computationally intensive, which can make it less practical for certain applications. There are many different factors that can affect the efficiency of MVECC, including the complexity of the mathematical operations involved, the size of the keys, and the hardware and software resources available [28-30]. By identifying and addressing these factors, it may be possible to improve the efficiency of MVECC and make it more practical for certain applications, such as grayscale image encryption. It is important to carefully evaluate any proposed improvements to MVECC or other cryptographic algorithms to ensure that they are effective and secure. It is also important to consider the trade-offs between efficiency and security, as increasing the efficiency of an encryption algorithm may come at the cost of reduced security [31].

One of the main challenges in image encryption is ensuring that the encrypted image is still visually similar to the original image, while also making it difficult for an attacker to decrypt the image without the appropriate key or keys [32-35]. This requires a balance between security and usability, as overly complex encryption methods may be difficult for users to implement or may result in heavily distorted or unusable images. Therefore, this work aims to propose a novel improvement to Menezes-Vanstone Elliptic Curve Cryptography to improve grayscale image encryption and decryption [36]. This proposed improvement to Menezes-Vanstone Elliptic Curve Cryptography (MVECC) aims to make the encryption and decryption of grayscale images more efficient by reducing the running time and

speeding up calculations. Finally, we used Entropy, Unified Average Changing Intensity (UACI), and Peak Signal to Noise Ratio (PSNR) to evaluate the efficiency of proposed scheme [37].

In this study, a new method for encrypting and decrypting grayscale images using Menezes-Vanstone Elliptic Curve Cryptography (MVECC) is proposed, which employs subtraction and addition instead of multiplication and inverse to make the mathematical calculations faster. ECC has various advantages over other approaches in terms of speed and power efficiency, which makes it appropriate for some applications such as image encryption. It requires less memory, fewer computations, and has a smaller key size [21]-[23].

2. LITERATURE REVIEW

Cryptography is a mathematical technique for ensuring secure image sharing over a non-secure channel. Elliptic curve cryptography (ECC) was proposed by Miller [1] and Koblitz [2], and it is one of the most efficient public key cryptography algorithms. ECC is a type of public key cryptography that is based on the mathematical concept of an elliptic curve. It was first proposed by Miller [1] and Koblitz [2] in the mid-1980s and has since become one of the most widely used public key cryptography algorithms. In ECC, the keys are derived from points on an elliptic curve, which is a curve defined by an equation of the form $y^2 = x^3 + ax + b$. The encryption and decryption of messages is performed using mathematical operations on these points. One of the main advantages of ECC is that it can provide strong security with relatively small keys. This makes it well-suited for use in applications where key size is a concern, such as in wireless communication or on devices with limited storage space [38-40]. ECC is also relatively efficient, which makes it practical for use in a wide range of applications. ECC is used in a variety of applications, including secure communication, digital signatures, and key exchange. It is also used in many standardized cryptographic protocols, such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL),

which are commonly used to secure internet communication [41-43].

In comparison with other systems like Rivest-Shamir-Adleman (RSA), ECC is generally considered to be more efficient than other public key cryptography algorithms, such as RSA, in terms of key size, memory requirements, and power usage [3], [4]. RSA is a widely used public key cryptography algorithm that is based on the difficulty of factoring large integers. RSA requires larger keys to achieve the same level of security as ECC, and it tends to be more computationally intensive, which can result in higher memory and power requirements. In ECC, a key size of 160 bits is identical to RSA's key size of 1024 bits. ECC is extensively utilized because of its advantages of faster computations, less storage capacity, and lower power consumption [5], [6]. Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC) was a well-known ECC scheme that provided good security for images and data [7]. MVECC is a cryptosystem that has no analogue for the discrete logarithm problem; this means that it does not depend on discrete logarithm problem. Therefore, the sender does not need to embed the plaintext on the EC but only mask it. MVECC is more efficient than other techniques because it just replaces each character with an ordered pair that is not required to be a point on E with no need for mapping [8]. Overall, ECC is generally considered to be more efficient than RSA, and it is often used in applications where efficiency is a concern. However, it is important to carefully evaluate the trade-offs between efficiency and security when choosing a cryptographic algorithm, as different algorithms may be more suitable for different applications [44-47].

Based on the literature, there have been many studies that have aimed to modify the MVECC approach in order to improve its efficiency, security, or other aspects. Some examples of these modifications include:

- Adding additional layers of encryption: Some studies have proposed using multiple layers of

encryption in MVECC, in order to increase the security of the system. This can be achieved by encrypting the message with multiple keys and ciphers, or by using additional cryptographic algorithms in conjunction with MVECC [48].

- Optimizing the implementation: Other studies have focused on optimizing the implementation of MVECC, in order to reduce the computational overhead and improve the efficiency of the system. This can be achieved through techniques such as optimizing the algorithms used, using hardware acceleration, or using more efficient data structures [49].

- Enhancing the security: Some researchers have proposed modifications to MVECC that aim to enhance the security of the system. This can be achieved through techniques such as adding additional security measures, such as authentication or integrity checks, or by using more advanced cryptographic techniques [50-55].

- Adapting MVECC to specific applications: Other studies have focused on adapting MVECC to specific applications, such as image encryption, in order to improve its effectiveness in these contexts. This can involve modifying the algorithms or key sizes used, or adapting the encryption process to the specific requirements of the application [56-60].

Several studies have been presented by many researchers to modify Menezes-Vanstone ECC approach. For instance, [52-54] introduced a new MVECC approach. They used the inverse operation only once and made the system safer and more confusing than the original algorithm [8]. Sagheer (2012) [8] presented three elliptic curve-based approaches. He was able to minimize computation time in comparison to the original approach by using a multiplication operation instead of an inverse operation [9]. Kurt and Yerlikaya (2013) proposed a new cryptosystem by using hexadecimal. They added additional features to Menezes-Vanstone ECC method by dividing the plaintext into blocks of one character, and then converted each character to one point

without using a mapping table [10]. Al-Saffar, et al. (2013) developed three techniques for encryption using Menezes-Vanstone Elliptic Curve Cryptosystem. The new methods minimized the inverse operations in decryption process and decreased the amount of time needed for encryption and decryption, but still depend on inverse and multiplication operations [11]. Dawahdeh, et al. (2016) proposed a new modification method for Menezes-Vanstone ECC and applied it on text messages by using hexadecimal ASCII code to make the encryption more difficult for hackers to attack [12]. Obaid and Al Saffar (2020) proposed a new method to encode image by dividing it into blocks of two numbers as an order pair [13]. In a recent study conducted by Ismail and Misro [29], they proposed cryptosystem combines Elliptic Curve Cryptosystem (ECC) with the Hill Cipher matrix, known as ECCHC, and adds an extra layer of security using cubic Bezier coefficient matrices. By combining ECC with the Hill Cipher matrix, it is possible to combine the efficiency and scalability of ECC with the simplicity and speed of the Hill Cipher. Adding an extra layer of security using cubic Bezier coefficient matrices can further increase the security of the system, making it more resistant to attacks. Banik et al., [30] discussed the limitations of a block-based image encryption scheme known as Abdelfatah's method. This method is based on both a chaotic system and elliptic curve cryptography (ECC), and it is used to encrypt images by dividing them into blocks and encrypting each block using a combination of chaotic and cryptographic techniques. One of the main drawbacks of Abdelfatah's method is that it may be vulnerable to certain types of attacks, such as known-plaintext attacks or chosen-plaintext attacks. These attacks can allow an attacker to retrieve the original image or partial information about the image by providing known or chosen plaintext blocks to the encryption algorithm. To solve this issue, the study [30] proposed algorithm is a block-based image encryption scheme that combines the use of an elliptic curve with a chaotic system. The elliptic curve component of the algorithm is based on a prime modulo with a

size of 512 bits, which is relatively large and can provide strong security. By combining the use of an elliptic curve with a chaotic system, the proposed algorithm may be able to provide strong security and resist certain types of attacks [61-65].

Security analysis is a critical step in determining the cryptographic technique's strength and efficiency [66-68]. Several measures (parameters) are used to analyze the efficiency of grayscale image encryption and compare the encrypted image with the original image in order to assess the encryption approach's performance [14], [15]. Various methods will be used in this paper to evaluate the encryption efficiency, for instance, Histogram Analysis, Entropy, Unified Average Changing Intensity (UACI), Peak Signal to Noise Ratio (PSNR), and Number of Pixels Change Rate (NPCR). Even though these are not the only security level measurements available, they are regarded standard metrics for evaluating image security level [16]-[20].

In this study, a new method for encrypting and decrypting grayscale images using Menezes-Vanstone Elliptic Curve Cryptography (MVECC) is proposed, which employs subtraction and addition instead of multiplication and inverse to make the mathematical calculations faster. ECC has various advantages over other approaches in terms of speed and power efficiency, which makes it appropriate for some applications such as image encryption. It requires less memory, fewer computations, and has a smaller key size [21]-[23].

3. MENEZES-VANSTONE ELLIPTIC CURVE CRYPTOSYSTEM (MVECC)

MVECC is a technique that does not depend on discrete logarithm problem like ElGamal cryptosystems. Therefore, sender does not need to embed the plaintext on the EC but only mask it [8], [24]. MVECC, or multi-vector encryption with cipher concatenation, is a variant of the ElGamal scheme that uses multiple keys and ciphers to encrypt and decrypt messages. In MVECC, the message is broken into two parts and each part is encrypted with a different key. This

makes it more difficult for an attacker to decrypt the message, as they would need to find both keys in order to retrieve the original message.

Both sender and receiver should agree on the elliptic curve $E(F_p)$ and the base point G before transmitting a message $M = (m_1, m_2)$ from user A to user B. Each user selects his private key at random from the interval $[1, n]$, with d for user A and e for user B, then multiplies the base point G with his private key to get the public key ($P_A = d.G$ and $P_B = e.G$, respectively). The secret key K is obtained by multiplying the private key of each party with the public key of the other party [25], [26]

$$K = e.P_A = d.P_B = d.e.G = (k_1, k_2)$$

(1)

Then ciphers the message by calculating

$$c_1 = m_1 * k_1 \text{ mod } p$$

(2)

$$c_2 = m_2 * k_2 \text{ mod } p$$

(3)

And sends $\{P_A, (c_1, c_2)\}$ to user B.

To decrypt (c_1, c_2) , user B multiplies his private key e by P_A to get the secret key $K = e.P_A = e.d.G = (k_1, k_2)$, then computes the following

$$m_1 = c_1 * k_1^{-1} \text{ mod } p$$

(4)

$$m_2 = c_2 * k_2^{-1} \text{ mod } p$$

(5)

to get the original message $M = (m_1, m_2)$ [27], [28].

MVECC is an effective and secure method of defending against attacks because any opponent can only see P_A and P_B , and they won't be able to retrieve the message M without getting the private keys d and e .

4. THE MODIFIED CRYPTOSYSTEM

This section introduces the Modification of Menezes-Vanstone Elliptic Curve Cryptosystem (MMVECC). This improvement makes the proposed technique more efficient than the original approach and other proposed techniques by speeding up the computations, because in encryption and decryption operations, the inverse operation is never used. When sending a message M from user A to user B, each user must choose a

random number from the interval $[1, p - 1]$ as a private key, n_A for user A and n_B for user B. The secret key $K = (x, y)$ is generated by multiplying the private key of each user with the public key of the other user

$$K = n_A \cdot P_B = n_B \cdot P_A = n_A \cdot n_B \cdot G = (x, y) \tag{6}$$

Equation (6) is describing a key exchange algorithm, in which two parties, A and B, can exchange a secret key using their respective public keys and a common point on an elliptic curve, G. In this equation, each party, A and B, has a private key, n_A and n_B , respectively, and a public key, P_A and P_B , respectively. The public keys are derived from the private keys and the common point G using an elliptic curve equation. Both parties should now have the same key, K, which they can use to securely communicate with each other.

Assume that user A wants to send user B a grayscale image. To begin encryption, user A converts every pixel value in the image to hexadecimal number of two digits $(h_1 h_2)_{16}$, then splits the number into two parts $(h_1, h_2)_{16}$, and each part is converted to decimal value d_1 and d_2 , respectively. Now, computes the ciphertext numbers (c_1, c_2) as follows

$$c_1 = (d_1 + x + y) \text{ mod } p \tag{7}$$

$$c_2 = (d_2 + c_1) \text{ mod } p \tag{8}$$

Equation (7) describes an encryption operation in which a message, d_1 , is encrypted using two keys, x and y , and a prime modulus, p . In this operation, the message d_1 is transformed into an encrypted form, c_1 , by adding it to the keys x and y and taking the remainder of the result when divided by the prime modulus p . The resulting cipher-text, c_1 , is dependent on the values of the message d_1 , the keys x and y , and the prime modulus p . To decrypt the message, the recipient would need to know the values of the keys x and y , as well as the prime modulus p , in order to reverse the encryption operation and recover the original message. Also, equation (8)

calculates the encrypted value c_2 by adding the message d_2 to the encrypted message c_1 .

Then calculates the encrypted pixel value by using the formula

$$B(1,1) = \text{mod}(c_1, 16) * 16 + \text{mod}(c_2, 16) \tag{9}$$

and sends $B(1,1)$ to user B.

User B starts decryption process by converting the value $B(1,1)$ to hexadecimal value $(h_1 h_2)_{16}$, then separates it to $(h_1, h_2)_{16}$ and converts them to decimal values $(x_1, x_2)_{10}$ and performs the following computations to get d_1 and d_2

$$c_1 = x_1 * 16 + x_2 \tag{10}$$

$$c_2 = x_1 * 16 + x_2 \tag{11}$$

$$d_1 = (c_1 - x - y) \text{ mod } p \tag{12}$$

$$d_2 = (c_2 - c_1) \text{ mod } p \tag{13}$$

Then, to recover the original pixel value use the formula

$$E(1,1) = d_1 * 16 + d_2 \tag{14}$$

Repeat the same processes for each pixel value in the grayscale image.

5. RESULTS AND DISCUSSION

In this section, the suggested approach MMVECC is used to apply encryption and decryption operations to various grayscale images of size 256×256 and the results are analyzed and explained.

Suppose that users A and B decided to use the elliptic curve function

$$E: y^2 \equiv x^3 + 17x + 33 \text{ (mod } 107)$$

So, the parameters domain for $E_{107}(17, 33)$ are $\{p, G, A, B\} = \{107, (5, 55), 17, 33\}$ [10].

Example: Suppose user A wants to encrypt and send 256×256 Cameraman grayscale image to user B. Then, as shown in the following steps, both will apply the suggested approach MMVECC to all image pixel values.

Step 1: Keys Creation

User A

1. Select $n_A = 27 \in [1, 106]$ as private key.
2. Calculate the public key $P_A = n_A \cdot G = 27(5, 55) = (45, 63)$.

User B

1. Select $n_B = 19 \in [1, 106]$ as private key.
2. Calculate the public key $P_B = n_B \cdot G = 19(5, 55) = (73, 13)$.

P_A and P_B are the public keys that will be exchanged between User A and User B.

Step 2: Encryption Process (done by user A)

1. Each pixel value in Cameraman image as shown in Table 1 is converted to hexadecimal value of two digits $(h_1 h_2)_{16}$.

Table 1. Cameraman image pixels in Decimal

A	1	2	3	4	5	6	7	8	---
1	169	168	174	175	177	177	181	179	---
2	174	175	176	173	180	179	179	177	---
3	171	178	172	177	177	178	180	182	---
4	170	173	177	171	178	178	183	181	---
:	:	:	:	:	:	:	:	:	---

The first value 169 will be converted to $(A9)_{16}$.

2. $(A9)_{16} \rightarrow (A, 9)_{16} \rightarrow (10, 9)_{10} = (d_1, d_2)_{10}$
3. The secret key is $K = n_A \cdot P_B = 27(73, 13) = (60, 48)$, then multiply the key K by a random number between 1 and $p - 1$; $r = 69$, to get $K = 69(60, 48) = (96, 86) = (x, y)$.
4. $c_1 = d_1 + x + y = (10 + 96 + 86) \bmod 107 = 192 \bmod 107 = 85$

5. $c_2 = d_2 + c_1 = (9 + 85) \bmod 107 = 94 \bmod 107 = 94$
6. Compute the value of the encrypted pixel by using the formula

$$B(1,1) = \bmod(c_1, 16) * 16 + \bmod(c_2, 16)$$

$$= \bmod(85, 16) * 16 + \bmod(94, 16) = 5 * 16 + 14 = 94$$

Repeat the same process for all 256×256 pixels to get the encrypted image pixels as shown in Table 2.

Table 2. Encrypted pixels for Cameraman image

B	1	2	3	4	5	6	7	8	---
1	94	59	134	21	222	1	227	208	---
2	100	254	119	218	123	54	156	86	---
3	148	172	81	86	103	2	174	74	---
4	215	224	1	165	2	172	144	39	---
:	:	:	:	:	:	:	:	:	---

Step 3: Decryption Process (done by user B)

1. $K = n_B \cdot P_A = 19(45, 63) = (60, 48)$, then multiply the value of K by the same random number $r = 69$ to get the secret key $K = 69(60, 48) = (96, 86) = (x, y)$.
2. The first pixel in the decrypted image $B(1,1) = 94$ will be converted to hexadecimal $(5E)_{16}$ then divided into two decimal values $h_1 = 5$ and $h_2 = 14$ and the encrypted values computed as $c_1 = 5 \times 16 + 5 = 85$
 $c_2 = 5 \times 16 + 14 = 94$
3. $d_1 = (c_1 - x - y) \bmod p = (85 - 96 - 86) \bmod 107 = -97 \bmod 107 = 10$

4. $d_2 = (c_2 - c_1) \bmod p = (94 - 85) \bmod 107 = 9 \bmod 107 = 9$
5. Compute the value of the decrypted pixel by using $E(1,1) = d_1 * 16 + d_2 = 10 * 16 + 9 = 169$.

Repeat the same process for all 256×256 encrypted pixels to get the original image pixels.

Figure 1 shows 256×256 Cameraman original grayscale image, encrypted and decrypted images with their histograms after encryption and decryption processes are applied by MMVECC.


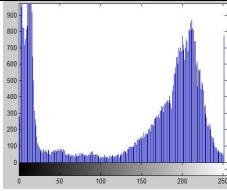
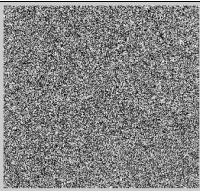
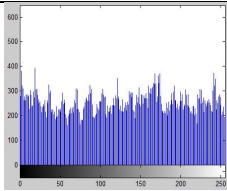

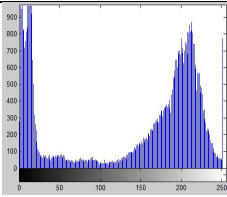
Cameraman 256 × 256	Image	Histogram
Original image		
Encrypted image		
Decrypted image		

Figure 1. The Original Image, Encrypted Image, And Decrypted Image With Their Histograms For Cameraman Image By MMVECC.

Table 3 shows the security measures for Cameraman grayscale image that are calculated during encryption and decryption processes.

Table 3. Security Measures For Cameraman Image By MMVECC

Entropy	PSNR	UACI	NPCR (%)
7.9818	7.0293	35.7763	100

The results of using MMVECC on different grayscale images of size 256×256 are summarized in Table 4. The entropy values are closed to the theoretical and ideal value, which is 8.

Table 4. MMVECC Security Measures For Some Images

The image	Entropy	PSNR	UACI	NPCR (%)
Cameraman	7.9818	7.0293	35.7763	100
Lena	7.9934	9.1265	28.5747	100
Einstein	7.9724	9.8101	26.3191	100
Smandril	7.9949	9.4907	27.6926	100

PSNR value assesses image encryption technique's performance. Table 4 shows that the PSNR values are low, indicating that the proposed technique is effective. The low PSNR value implies original and encrypted images are not identical; indicating that the encryption approach is effective.

Table 4 also contains UACI values, which are used to determine the difference between the ciphered and original images. The anticipated value for UACI for 256×256 grayscale images is 33.46. Table 4 demonstrates that the UACI values are near to the predicted value 33.46, and the variation in results related to the image format and size. So, the proposed approach is resistant to different types of attacks.

Finally, Table 4 displays the NPCR values obtained from applying MMVECC on a variety grayscale images. NPCR is another parameter used to determine the difference between the original and deciphered image. Table 4 shows that the NPCR values are higher than expected and close to the ideal value 100, and this indicates that the proposed technique is resistant to different attacks.

Another comparison between the proposed technique MMVECC and some other techniques

for Cameraman grayscale image of size 256×256 is shown in Table 5. Entropy evaluates the security of the ciphertext image and represents the strength of the uncertainty of the image information. It is clear that the Entropy value of the proposed technique is higher than the values of the other techniques except Hanif, et al. (2022) and it is nearest to the theoretical value eight. Entropy value indicates that our method can effectively resist statistical analysis attacks. PSNR value in the proposed technique is also less and better than the values of Hanif, et al. (2022) and Panduranga, et al. (2012) techniques. UACI value in the proposed technique is good comparing with the other techniques and it's near the expected value 33.46, so our encryption algorithm has good sensitivity to plaintext. Also, the NPCR value in the proposed technique is 100% and it is exceeded the expected values, it is higher and better than the values of the other techniques, and this indicates that the original image and the decrypted image are completely identical in the proposed technique. So, Table 5 shows that the proposed technique is more efficient and has higher security than the other techniques and resistant against different attacks.

Table 5: The Entropy, PSNR, UACI, And NPCR For Cameraman Image

The Method	Cameraman Image (256 × 256)			
	Entropy	PSNR	UACI	NPCR (%)
The proposed technique MMVECC	7.9818	7.0293	35.7763	100
Beg, et al. (2022) [31]	7.9716	NA	33.2151	99.5987
Liu, et al. (2022) [32]	7.9581	NA	33.3015	99.5739
Hanif, et al. (2022) [33]	7.9952	7.7515	33.6619	99.6445
Wang, et al. (2019) [34]	7.9773	NA	32.7981	99.5897
Sheela, et al. (2018) [35]	7.9990	7.7743	32.2914	99.6109
Panduranga, et al. (2012) [36]	7.7344	8.3628	34.4	99.5987
Expected values	8	Minimum value is better	33.46	99.61

Figure 2 shows the entropy values for **Cameraman** grayscale image by using the proposed MMVECC and some other techniques.

It is clear from the figure that the entropy value in the proposed algorithm is approximately equal the expected and theoretical value eight.

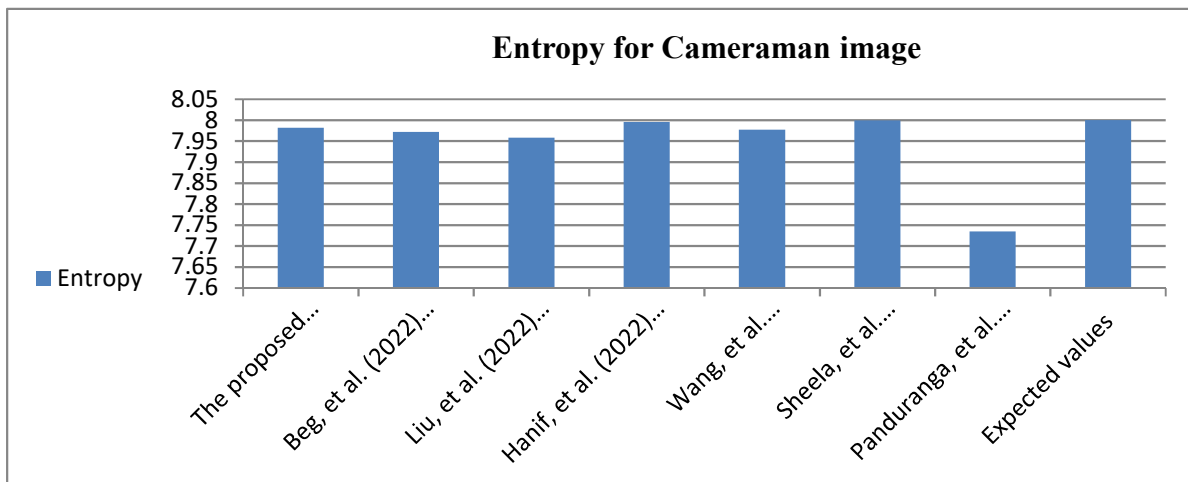


Figure 2: Entropy Values For **Cameraman** Image By Different Techniques

Figure 3 shows PSNR values for **Cameraman** grayscale image by using the proposed MMVECC, Hanif, et al. (2022), Sheela, et al. (2018), and Panduranga, et al. (2012) techniques. PSNR value in the proposed

technique is less than values of the other techniques, which indicates that the proposed algorithm is better than others in resisting the adversaries.

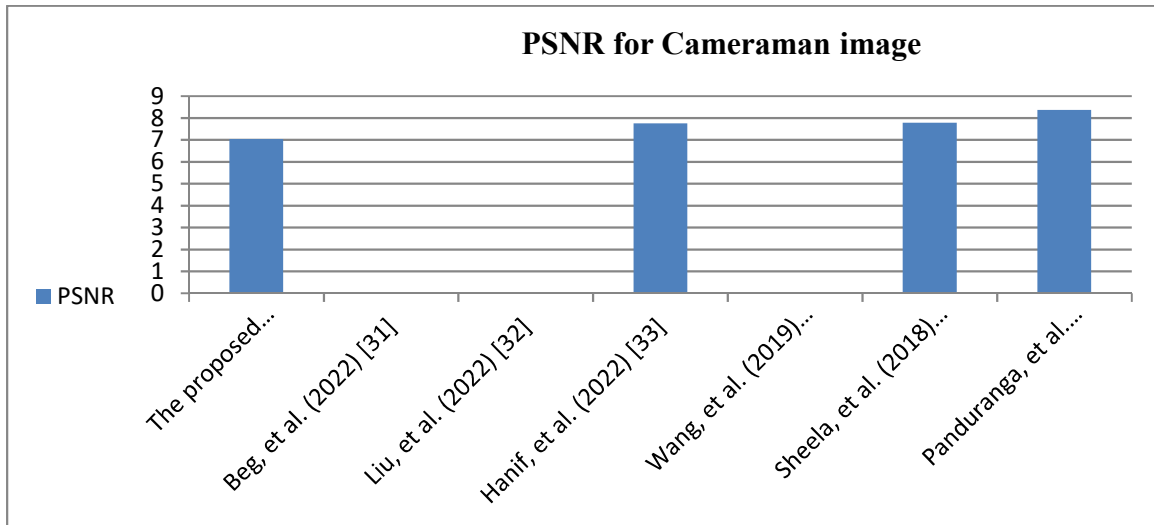


Figure 3: PSNR Values For *Cameraman* Image By Different Techniques

Figure 4 shows NPCR values for *Cameraman* grayscale image by using the proposed MMVECC and some other techniques. NPCR in the proposed technique is 100% and this

indicates that the original image and the decrypted image in the proposed technique are completely identical, which leads to the efficiency of the proposed cryptography technique.

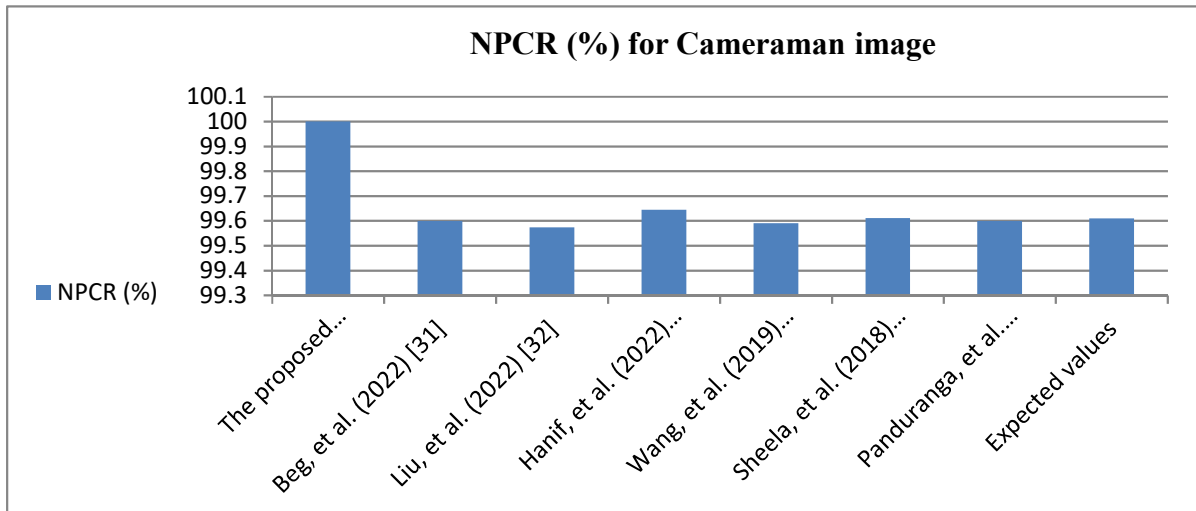


Figure 4: NPCR Values For *Cameraman* Image By Different Techniques

5. CONCLUSION

In this research, an efficient technique for encrypting and decrypting grayscale images is proposed in order to improve security and reduce the time consumed in mathematical calculations.

Elliptic Curve Cryptography is one of the most efficient encryption and decryption techniques and secures against attacks since it is based on the elliptic curve discrete logarithm problem, which is difficult for adversaries to solve. When compared to other cryptography techniques with similar

levels of security, such as RSA, ECC's short key size provides enhanced security.

To improve Menezes-Vanstone Elliptic Curve Cryptosystem for grayscale images, a new efficient technique (MMVECC) has been developed. It reduced the amount of time encryption and decryption procedures needed to complete. Because inverse and multiplication operations require more calculation time, only addition and subtraction operations are used in the proposed method, which speeds up mathematical computations and reduces running time. Table 3 shows that the proposed method on Cameraman grayscale image produces significant results in terms of Entropy, PSNR, UACI, and NPCR. The proposed method's Entropy value 7.9818 is closest to the predicted value 8. The PSNR value 7.0293 is low, indicating that the proposed approach is effective. In addition, the UACI value 35.7763 is the most similar to the expected value. Table 4 reveals positive findings for Lena, Einstein, and Smandril images, demonstrating the efficacy of the proposed technique.

Because the proposed approach has simple structure and speedier computations, it may be employed efficiently in several applications such as e-commerce, embedded systems, chip cards, smart cards, PDAs, and portable devices.

ACKNOWLEDGMENT

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. Grant No. 6051).

REFERENCES

- [1] V. S. Miller, Use of elliptic curves in cryptography, *Advanced in Cryptology, Proceedings of Crypto85, Lecture note in Computer Science*, v. 218, Springer Verlag, pp. 417-426, 1986.
- [2] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, 48 (1987), 203-209.
- [3] Ali, A., Almaiah, M. A., Hajje, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, 22(2), 572.
- [4] Almaiah, M. A., & Al-Khasawneh, A. (2020). Investigating the main determinants of mobile cloud computing adoption in university campus. *Education and Information Technologies*, 25(4), 3087-3107.
- [5] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 international conference on information technology (ICIT) (pp. 779-786). IEEE.
- [6] Almaiah, M. A., Hajje, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. *Sensors*, 22(4), 1448.
- [7] Adil, M., Khan, R., Ali, J., Roh, B. H., Ta, Q. T. H., & Almaiah, M. A. (2020). An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. *IEEE Access*, 8, 163209-163224.
- [8] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. *Sensors*, 20(8), 2311.
- [9] Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A Conceptual Model for Investigating the Effect of Privacy Concerns on E-Commerce Adoption: A Study on United Arab Emirates Consumers. *Electronics*, 11(22), 3648.
- [10] Siam, A. I., Almaiah, M. A., Al-Zahrani, A., Abou Elazm, A., El Banby, G. M., El-Shafai, W., ... & El-Bahnasawy, N. A. (2021). Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications. *Computational Intelligence and Neuroscience*, 2021.
- [11] Almaiah, M. A., Ali, A., Hajje, F., Pasha, M. F., & Alohal, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. *Sensors*, 22(6), 2112.
- [12] Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., ... & Khan, R. (2020). Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. *IEEE Access*, 8, 176495-176520.

- [13] Alabadleh, A., Aljaafreh, S., Aljaafreh, A., & Alawasa, K. (2018). A RSS-based localization method using HMM-based error correction. *Journal of Location Based Services*, 12(3–4), 273–285.
- [14] Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of cyber security threats on mobile devices and applications. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications* (pp. 107-123). Cham: Springer International Publishing.
- [15] Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV based mutual authentication scheme for constraint oriented networks. *IEEE Access*, 8, 44459-44469.
- [16] Almomani, O., Almaiah, M. A., Alsaaidah, A., Smadi, S., Mohammad, A. H., & Althunibat, A. (2021, July). Machine learning classifiers for network intrusion detection system: comparative study. In *2021 International Conference on Information Technology (ICIT)* (pp. 440-445). IEEE.
- [17] Adil, M., Khan, R., Almaiah, M. A., Binsawad, M., Ali, J., Al Saaidah, A., & Ta, Q. T. H. (2020). An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. *IEEE Access*, 8, 148510-148527.
- [18] Alsyouf, A., Lutfi, A., Al-Bsheish, M., Jarrar, M. T., Al-Mugheed, K., Almaiah, M. A., ... & Ashour, A. (2022). Exposure detection applications acceptance: The case of COVID-19. *International Journal of Environmental Research and Public Health*, 19(12), 7307.
- [19] Bubukayr, M. A. S., & Almaiah, M. A. (2021, July). Cybersecurity concerns in smart-phones and applications: A survey. In *2021 international conference on information technology (ICIT)* (pp. 725-731). IEEE.
- [20] Almaiah, M. A. (2021). A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In *Artificial intelligence and blockchain for future cybersecurity applications* (pp. 217-234). Cham: Springer International Publishing.
- [21] Alese, B. K., Philemon E. D., Falaki, S. O., Comparative Analysis of Public-Key Encryption Schemes, *International Journal of Engineering and Technology* Volume2 No. 9, 2012.
- [22] Rajadurga, K., and S. Ram Kumar. "GF (2m) Based Low Complexity Multiplier for Elliptic Curve Cryptography Systems." *Networking and Communication Engineering* 6, no. 4 (2014): 150-155.
- [23] Alamer, M., & Almaiah, M. A. (2021, July). Cybersecurity in Smart City: A systematic mapping study. In *2021 international conference on information technology (ICIT)* (pp. 719-724). IEEE.
- [24] Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Hwaitat, A. K. A., ... & Aldhyani, T. H. (2022). Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels. *Electronics*, 11(21), 3571.
- [25] Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-Khasawneh, A., & Khawatreh, S. (2020). A new hybrid text encryption approach over mobile ad hoc network. *Int. J. Electr. Comput. Eng.(IJECE)*, 10(6), 6461-6471.
- [26] Alrawad, M., Lutfi, A., Alyatama, S., Elshaer, I. A., & Almaiah, M. A. (2022). Perception of occupational and environmental risks and hazards among mineworkers: A psychometric paradigm approach. *International journal of environmental research and public health*, 19(6), 3371.
- [27] Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., ... & Aldhyani, T. H. (2022). Investigating the effect of perceived security, perceived trust, and information quality on mobile payment usage through near-field communication (NFC) in Saudi Arabia. *Electronics*, 11(23), 3926.
- [28] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics*, 11(20), 3330.
- [29] Albalawi, A. M., & Almaiah, M. A. (2022). Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. *J. Theor. Appl. Inf. Technol.*, 100, 2988-3011.
- [30] Alves, J., & Pinto, A. (2018). On the use of the blockchain technology in electronic voting systems. *International Symposium on Ambient Intelligence*, 323–330.
- [31] Bulut, R., Kantarci, A., Keskin, S., & Bahtiyar, S. (2019). Blockchain-Based Electronic Voting System for Elections in

- Turkey. UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering, 183–188. <https://doi.org/10.1109/UBMK.2019.8907102>
- [32] Cash, M., & Bassiouni, M. (2018). Two-tier permission-ed and permission-less blockchain for secure data sharing. 2018 IEEE International Conference on Smart Cloud (SmartCloud), 138–144.
- [33] Qasem, M. H., Obeid, N., Hudaib, A., Almaiah, M. A., Al-Zahrani, A., & Al-Khasawneh, A. (2021). Multi-agent system combined with distributed data mining for mutual collaboration classification. *IEEE Access*, 9, 70531-70547.
- [34] Almudaires, F., & Almaiah, M. (2021, July). Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In 2021 International Conference on Information Technology (ICIT) (pp. 732-738). IEEE.
- [35] AlMedires, M., & AlMaiah, M. (2021, July). Cybersecurity in industrial control system (ICS). In 2021 International Conference on Information Technology (ICIT) (pp. 640-647). IEEE.
- [36] Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., ... & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using sem. *Sustainability*, 15(13), 9908.
- [37] Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. *Electronics*, 12(17), 3618.
- [38] Fu Minfeng and Chen Wei, Elliptic curve cryptosystem EIGamal encryption and transmission scheme, International Conference on Computer Application and System Modeling (ICCASM 2010), 978-1-4244-7237-6/10 ©2010 IEEE. DOI: 10.1109/ICCASM.2010.5620105
- [39] Dawahdeh, Z. E., Yaakob, S. N., & bin Othman, R. R. (2018). A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. *Journal of King Saud University-Computer and Information Sciences*, 30(3), 349-355. <https://doi.org/10.1016/j.jksuci.2017.06.004>
- [40] A. Menezes, S. Vanstone, "Elliptic curve cryptosystem and their implementation", *Journal of cryptography* 6 (4), pp. 209 - 224, 1993. <https://doi.org/10.1007/BF00203817>
- [40] Sadiq, Ahmed Tariq, and Nasreen J. Kadhim. ENHANCED MENEZES-VANESTONE ELLIPTIC CURVES CRYPTOSYSTEM, *Journal of Al-Nahrain University*, Vol.12(1), March, 2009, pp.162- 165. DOI: 10.22401/JNUS.12.1.23
- [41] Ali M. Sagheer, Elliptic curves cryptographic techniques, *Proceeding of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS'2012)*, © 2012 IEEE, 12 - 14 December 2012, Gold Coast, Australia. DOI: 10.1109/ICSPCS.2012.6507952
- [42] Kurt, M., Yerlikaya, Y., A new modified cryptosystem based on Menezes Vanstone elliptic curve cryptography algorithm that uses characters' hexadecimal values, ISBN: 978-1-4673-5612-1©2013 IEEE. DOI: 10.1109/TAEECE.2013.6557316
- [43] Al-Saffar, Najlae F. Hameed, Md Said, and Mohamad Rushdan. "On the Mathematical Complexity and the Time Implementation of Proposed Variants of Elliptic Curves Cryptosystems." *International Journal of Cryptology Research* 4.1 (2013): 42-54.
- [44] Dawahdeh, Z. E., Yaakob, S. N., & Othman, R. R. B. (2016). A New Modification For Menezes – Vanstone Elliptic Curve Cryptosystem. *Journal of Theoretical and Applied Information Technology*, 85(3).
- [45] Obaid, Z. K., & Al Saffar, N. F. H. (2020). Image Encryption Based on Menezes Vanstone Elliptic Curve Cryptosystem. *Solid State Technology*, 63(3), 5256-5265.
- [46] Singh, L. D., & Singh, K. M. (2015a). Image encryption using elliptic curve cryptography. *Procedia Computer Science*, 54, 472-481. <https://doi.org/10.1016/j.procs.2015.06.054>
- [47] Jasra, B., & Moon, A. H. (2020, January). Image Encryption techniques: A Review. In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 221-226). IEEE. DOI: 10.1109/Confluence47617.2020.9058071
- [48] Kumar, M., Aggarwal, A., & Garg, A. (2014). A Review on Various Digital Image Encryption Techniques and Security Criteria. *International Journal of Computer Applications*, 96(13).

- [49] Singh, P. K., Alam, M. M., & Tyagi, S. (2015). Image Encryption Technique Based on Permutation and Combination. *International Journal of Computer Science and Mobile Computing*, 4(6), 1112-1120.
- [50] Salameh, J. N. B. (2016). An Investigation of the Use of MJEAs in Image Encryption. *WSEAS transactions on computers*. Volume 15.
- [51] Reyad, O., Mofaddel, M. A., Abd-Elhafiez, W. M., & Fathy, M. (2017, December). A novel image encryption scheme based on different block sizes for grayscale and color images. In *2017 12th International Conference on Computer Engineering and Systems (ICCES)* (pp. 455-461). IEEE. DOI: 10.1109/ICCES.2017.8275351
- [52] Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. *Sensors*, 20(18), 5162. <https://doi.org/10.3390/s20185162>
- [53] Dawahdeh, Ziad E., Shahrul N. Yaakob, and Ali Makki Sagheer. "Modified ElGamal Elliptic Curve Cryptosystem using Hexadecimal Representation." *Indian Journal of Science and Technology* 8.15 (2015).
- [54] Ali, M, Sagheer, Enhancement of elliptic curves cryptography methods, MSc. Thesis, University of Technology, Baghdad, Iraq, 2004.
- [55] Hongqiang Lv; Hui Li; Junkai Yi; Hao Lu, Optimal Implementation of Elliptic Curve Cryptography, International conference on service operations and logistics and informatics, 978-1-4799-0529-4©2013 IEEE. DOI: 10.1109/SOLI.2013.6611377
- [56] T. ElGamal. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." *IEEE Trans. On Information Theory* 31 vol.4, pp.469-472, 1985. DOI: 10.1109/TIT.1985.1057074
- [57] Diffie, W. and Hellman, "New Directions in Cryptography." *IEEE Trans. On Information Theory*, IT-22, vol.6, pp.644-654, 1976. DOI: 10.1109/TIT.1976.1055638
- [26] Obaid, Z. K., & Al Saffar, N. F. H. (2021). Image encryption based on elliptic curve cryptosystem. *International Journal of Electrical and Computer Engineering*, 11(2), 1293. DOI: 10.11591/ijece.v11i2.pp1293-1302
- [58] Obaid, Z. K., & Al Saffar, N. F. H. (2021). Image encryption based on elliptic curve cryptosystem. *International Journal of Electrical and Computer Engineering*, 11(2), 1293. DOI: 10.11591/ijece.v11i2.pp1293-1302
- [59] Hankerson, Darrel, Menezes, Alfred J., Vanstone, Scott, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.
- [60] William Stallings, *Cryptography and Network Security: Principles and Practices*, Seventh Edition, Pearson, 2017.
- [61] Ismail NH, Misro MY. An improved image encryption algorithm based on Bézier coefficients matrix. *Journal of King Saud University-Computer and Information Sciences*. 2022 Oct 17.
- [62] Banik A, Laiphrakpam DS, Agrawal A, Patgiri R. Secret image encryption based on chaotic system and elliptic curve cryptography. *Digital Signal Processing*. 2022 Sep 1;129:103639.
- [63] Beg, S., Baig, F., Hameed, Y., Anjum, A., & Khan, A. (2022). Thermal image encryption based on laser diode feedback and 2D logistic chaotic map. *Multimedia Tools and Applications*, 81(18), 26403-26423.
- [64] Liu, H., Liu, J., & Ma, C. (2022). Constructing dynamic strong S-Box using 3D chaotic map and application to image encryption. *Multimedia Tools and Applications*, 1-16.
- [65] Hanif, M., Iqbal, N., Ur Rahman, F., Khan, M. A., Ghazal, T. M., Abbas, S.,... & Yeun, C. Y. (2022). A novel grayscale image encryption scheme based on the block-level swapping of pixels and the chaotic system. *Sensors*, 22(16), 6243.
- [66] Wang, X., Çavuşoğlu, Ü., Kacar, S., Akgul, A., Pham, V. T., Jafari, S., ... & Nguyen, X. Q. (2019). S-box based image encryption application using a chaotic system without equilibrium. *Applied Sciences*, 9(4), 781.
- [67] Sheela, S. J., Suresh, K. V., & Tandur, D. (2018). Image encryption based on modified Henon map using hybrid chaotic shift transform. *Multimedia Tools and Applications*, 77, 25223-25251.
- [68] Panduranga, H. T., Kumar, H. S., & Kumar, S. N. (2012, December). Hybrid approach for dual image encryption using nibble exchange and Hill-cipher. In *Machine Vision and Image Processing (MVIP), 2012 International Conference on* (pp. 101-104). IEEE.