# Encryption and Decryption Techniques using MBECC for Image Data Transfer

**R.Sankarasubramanian**
Ph.D Research Scholar (Part-Time) & Associate Professor, Department of Computer Science,
Erode Arts and Science College (Autonomous), Erode, Tamil Nadu, India.
**Dr.S.Sukumaran**
Research Supervisor & Associate Professor, Department of Computer Science,
Erode Arts and Science College (Autonomous), Erode, Tamil Nadu, India.

**Abstract-Today, the market for mobile communication and personal digital assistance is growing rapidly. The mobile electronic payment is secure messaging have an inherent need for security. The data is safely encrypted cannot assure that the message or information being exchanged is not intercepted by intruders. The crucial data cannot be transmitted in the unmodified form since it can be easily hacked by intruders. Cryptography is art of sending secret messages between sender and receiver. In the second phase of this research, an image data block based technique has been proposed the classic technique of mapping the image blocks to affine points in the elliptic curve has been removed. The proposed image based technique is experimented with a standard input image. The performance of the proposed technique is evaluated in terms of entropy, encryption time and decryption time. The proposed Matrix Base Conversion Elliptic Curve Crypto (MBECC) technique is performed better when compared with the existing AES, CFES and MBC techniques.**
**Keywords- AES, CFES, MBC, MBECC,ECC.**

## 1. INTRODUCTION

Cryptography is commonly employed security is addressed by choosing a security protocol. The security protocols realize the objectives using appropriate cryptographic algorithms. In recent years, significant development in multimedia technologies in the transmission of multimedia data such as audio, video and images over the internet is now very common. Internet is a very insecure channel and these possess a number of security issues and to achieve confidentiality and security of multimedia data.

The processing and transmission of multimedia data over insecure networks, possesses several security problems. The multimedia data security has become a serious and major issue in telemedicine, military, E-Commerce, financial transaction and mobile phone applications. To provide security attributes to multimedia data needs to protect communicated information (plaintext) from unauthorized users. Multimedia data are needs to be secured from different type of attacks. Cryptography enables to transmit data across insecure networks it cannot be read by anyone except the authorized recipient.

## 2. RELATED WORKS

Akash et al. [1] compared data encryption standard and advanced encryption standard techniques on the basis of avalanche effect. The property of any encryption algorithm in which a small change in either the key or the plaintext should produce a significant change in the cipher text.

Chang-Mok et al., [2] presented an algorithm in multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique.

Guosheng et al., [3] described highly optimized image algorithm using permutation and substitution methods. In order to enhance the pseudorandom characteristics of chaotic sequences, an optimized treatment and a cross-sampling disposal is used.

Huang-Pei et al., [4] discussed the chaotic system generates a chaotic sequence, which was changed into a binary stream using a threshold function. The other chaotic system used to construct a permutation matrix. First using the binary stream as a key stream, randomly the pixel values of the images are modified. Then, modified image is encrypted again by permutation matrix.

Obaida et al., [5] developed a new approach for complex encrypting and decrypting Data maintains the security on the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption and decryption.

Kamali et al., [6] modified the advanced encryption standard to provide a high level security and better image encryption is higher than that of original AES encryption algorithm.

Maniccam et al., [7] developed a new algorithm for lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on patterns generated by the SCAN methodology. The SCAN is a formal language-based 2D spatial-accessing methodology generate a wide range of scanning paths or space filling curves.

Mohammad et al., [8] proposed a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks and using the transformation algorithm it was rearranged and Blowfish algorithm is used for encrypting the transformed image correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

Ravi et al., [9] proposed bit shifting and stuffing method stuffing a new bit in the place of unused bit which is shifting from another printable character. After the encryption bit shifting and stuffing for every 8 bytes of plain text it will

generate seven bytes cipher text and in decryption for every seven bytes of cipher text it will reproduce eight bytes of plaintext.

Santhosh et al., [10] proposed Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers algorithm contains two levels of Exclusive OR operation. The algorithm is useful in transmission of messages and data between one user and another.

Satyajeet et al., [11] presented a symmetric cryptographic algorithm for data encryption and decryption based on ASCII values of characters. The secret key is converted to another string is used as key to encrypt or decrypt the data.

Shashi et al. [12] analyzed RSA, DES and AES considering certain parameters are the major issue of concern in any Encryption Algorithm. From the results DES algorithm consumes least encryption time and AES algorithm has least memory usage and RSA consume longest encryption time and memory usage is also very high.

Zeghid et al., [13] analyze the Advanced Encryption Standard (AES) and in their image encryption technique they add a key stream generator to AES for ensuring the encryption performance.

## 3. Existing Methodology

The encryption and decryption techniques such as

### 3.1 Advanced Encryption Standard (AES)

The National Institute of Standards and Technology (NIST) adopted the Rijndael Algorithm as the Advanced Encryption Standard in 2001. This algorithm was invented by two Belgian scientists, Vincent Rijmen and Jon Daemen. The first round of the selection process was focused on the three main criteria that were evaluated to select a winner of the AES process were security, costs and its implementation characteristics (should be easily understood and implemented). The Advanced Encryption Standard has no weakness in its security. Its cost with regards to intellectual patent rights is free and implementation on hardware and software is cheapest among all the finalists. AES is versatile in that it can be implemented on both memory-bound hardware like 8-bit microcontrollers as well as dedicated hardware to provide real-time encryption of streaming data at processing rates reaching gigabits per second.

### 3.2 Data Encryption Standard

Data encryption standard is the most widely used method of data encryption using a secret key. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. It was developed in the 1970s by the National Bureau of Standards with the help of the National Security Agency. Its purpose is to provide a standard method for sensitive commercial and unclassified data. IBM created the first draft of the algorithm, calling it LUCIFER. DES officially became a standard in November of 1976. Data encryption algorithm has a 64-bit block size and uses a 56bit key during execution (8 parity bits are stripped of from the full 64-bit key). The DEA can also be used for single user encryption, such as to store files in a hard in encrypted form. NIST re-certifies DES every 5 years. DES has been in worldwide use for over 20 years, and due to the fact that it is a defined standard that any system implementing DES can communicate with any other system using is it.

## 4. Proposed MBECC Methodology

Information security is one of the most important issues now-a-days where information is sent from one to another place with rapid rates. Multitude use of digital data in the applications of medical, defense, military, banking and other multimedia channel leads the concept of authentication of digital data. So the best way of transferring huge amount of digital data is in form of image. Due to inherent property of image, such as huge information capacity and high correlation among pixels, it is selected for the encryption algorithms. There are many image encryption algorithms which utilized chaotic map, logistic map, advance encryption standard, Arnold map, affine transformation, Fourier transform and fractional Fourier transform. Researcher finished the purpose of encryption by scrambling the image pixels only, some have changed the spatial domain of image to frequency domain by using Fourier transform. The extension of Fourier transform is fractional Fourier transform which is also applied in large extent in the field of image encryption. These techniques do not fulfill the requirements of the authenticity of the image against malicious users. Recently, Linear Canonical transform is applied multitude in the field of double image encryption process due to its inherent property.

The primary goal is to provide security of images which is travelling over internet. Moreover, an image-based data requires more effort during encryption and decryption. In this work, enhanced technique has been developed for mapping the image using Matrix Base Elliptic Curve Cryptography (MBECC) analysis the entropy and correlation between pixels value of various image encryption algorithm. The need to develop new encryption schemes comes from the fact that traditional encryption schemes for textual data are not suitable for multimedia data stream. This paper presents a framework to evaluate image encryption schemes proposed. MBECC considered the input plain image into ASCII values. In this algorithm the input image is first converted into its ASCII values. It performs a string manipulation algorithm which will change the relative position of atomic data values by reversing them. Here, divide the string into square matrices of maximum possible order and then add magic square matrix of same size is considered. The base conversion is performed on the basis of key which is calculated by the size of square matrix generated. The base conversion is also performed on the remaining elements which could not be containing in the square matrices. The experimental result shows that MBECC provides better for encrypting and decrypting for digital images when compared with the existing methods AES and DES.

### 4.1 Image Encryption

Image encryption is the process of encoding image in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the image is encrypted using an encryption algorithm, turning it into an unreadable image. This is usually done with the use of

encryption keys, which specifies how the image is to be encoded. Any adversary that can see the encrypted image should not be able to determine anything about the original image. An authorized party, however, is able to decode the encrypted image using a decryption algorithm. That usually requires a secret decryption key, so adversaries do not have access.

The technique of converting a given number from one number system to another by means of simple calculations is known as Matrix Base Conversion. A square matrix in which the sum of all elements in each column and in each row is same is called Magic Square matrix. To calculate the sum use the formula (r* ($r^2$+1))/2, where r is the size of square matrix. A square matrix order refers to a matrix with equal number of rows and columns.

This new proposed block encryption algorithm is block cipher. It divides data into blocks of pixels of equal length. Some blocks of pixels are selected and the only selected blocks of pixels are encrypted using a special mathematical set of functions known as key. Symmetric key technique is used in this algorithm for both encoding and decoding i.e. same key is used at both ends. Some additional tasks are performed to provide strong security to this algorithm like shuffling. There is another plus point of this algorithm is that it protects the cipher image from unauthorized access such as Brute-force as selection process is applied and the key is changed many times in the encryption process. It will be very hard to attain original image from cipher image.

### 4.2 Elliptic Curve Cryptography

The basic idea of Elliptic Curve Cryptography (ECC) and its implementation through co-ordinate geometry for data encryption. The implementation of ECC on two finite fields, prime field and binary field. An overview of ECC implementation on two dimensional representations of plaintext coordinate systems and data encryption technique. Much attention given to the mathematics of elliptic curves starting with their derivations and the proof of how points upon them form an additive abelian group for cryptographic purposes, specifically results for the group formed by an elliptic curve over a finite field can form public key cryptographic systems for encryption and key exchange. The algorithm is mainly based on scan patterns depicted. The steps formed the new image encryption. The 128-bit key is gradually explained and formed during each step implemented by gray scale images.

## 5. ALGORITHM

The process of the image retrieval takes place in two phases and defined as algorithm I and II.

**Algorithm I**

**//** Algorithm for Key Generation **//**

***Step 1:*** *Initialize the key*
***Step 2:*** *Select E (a,b) with an elliptic curve over GF(p) or GF(2n).*
***Step 3:*** *Select a point on the curve e1= (x1, y1).*
***Step 4:*** *Select d*
***Step 5:*** *Calculate e2= (x2, y2) = d * e1*
***Step 6:*** *Announce e1, e2 as public key and keep "d" as key.*
***Step 7:*** *End*

***Algorithm II***

**//** Algorithm for Encrypting Image **//**
**Input: Plain image**
**Output: Cipher image**

***Step 1:*** *Load an input image.*
***Step 2:*** *Procedure random key ( )*
*{*
*Convert into ASCII value*
*then*
*Convert binary values into random values*
*Store as base key*
*}*
***Step 3:*** *A new key is generated every time on cipher image.*
***Step 4:*** *Initialize I=0 in encrypted process*
***Step 5:*** *Procedure image blocks ( )*
*{*
*Step 1 : input M, N //size of input image*
*Step 2 : input p,q //p,q ← horizontal and vertical Blocks//*
*Step 3 : assign q ←0, p ←0*
*Step 4 : for i = 1 to M*
*for j=1 to N*
*{*
*HNB = int (Image width/10)*
*VNB = int (Image Height/10)*
*}*
*Step 5 : Establish the horizontal and vertical blocks of the input image*
*Step 6 : Return*
*}*
***Step 6:*** *Extract images with the same size as the original image*
***Step 7:*** *Construction key-image and encrypted image.*
***Step 8:*** *Save as the key-image and encrypted images.*
***Step 9:*** *Reverse the decrypted process*
***Step 10:*** *Construct and display the decrypted image.*

***Algorithm III***

**//** Algorithm for Decrypting Image **//**
**Input: Cipher image**
**Output: Plain image**

***Step 1:*** *Load an input image.*
***Step 2:*** *Extract images with the same size as the original image*
***Step 3:*** *Construction key-image and decrypted image.*
***Step 4:*** *Initialize I=0 in decrypted process*
***Step 5:*** *Procedure image blocks ( )*
*{*
*Step 1 : input M, N //size of input image*
*Step2 : input p,q*
*Step 3 : assign q ←0, p ←0*
*Step 4 : for i = 1 to M*
*for j=1 to N*
*{*
*HNB = int (Image width/10)*
*VNB = int (Image Height/10)*
*}*
*Step 5 : Establish the horizontal and vertical blocks of the input image*
*Step 6 : Return*
*}*
***Step 6:*** *Procedure random key ( )*
*{*
*Convert into ASCII value*
*then*
*Convert binary values into random values*

*Store as base key*
*}*

***Step 7:*** *A new key is generated every time on plain image.*
***Step 8:*** *Save as the key-image and decrypted images.*
***Step 9:*** *Reverse the decrypted process*
***Step 10:*** *Construct and display the decrypted image.*

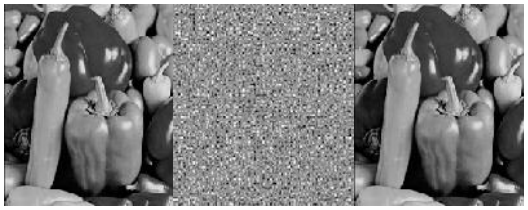
## 6. Experiments and Results

The proposed method is experimented with a different types of images are processed using MATLAB. The table 5.1 shows the comparison values of Entropy values. The algorithm was applied on a bit mapped (bmp) image that size. To evaluate the impact of the insertion process on the encrypted images, three different cases were tested. The horizontal number of blocks and the vertical number of blocks is 1024 blocks. Therefore, the number of bits that need to be sent within the encrypted image will be 20 bits 10 bits for horizontal number of blocks and 10 bits for vertical number of blocks. These 20 bits will be inserted in the image data randomly based on the secret key by using the LSB insertion. Hence the encrypted images with and without insertion position of data. The experimentation is carried out by MATLAB. It stands for MATrix LABoratory. MATLAB® is a high-performance language for technical computing. It integrates computation, visualization and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. Typical uses include Math and computation Algorithm development Data acquisition Modeling, simulation and prototyping Data analysis, exploration and visualization Scientific and engineering graphics Application development, including graphical user interface building.

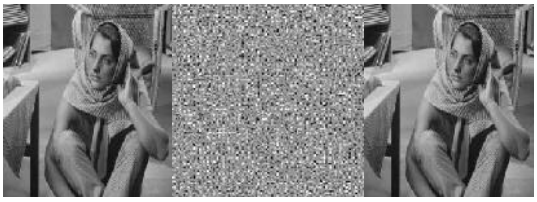
In order to evaluate the performance of the proposed system with the existing system the Entropy Values, Mean Square Error and Block Size are computed with the selective image sets. The obtained results of the image with the proposed model is tabulated in the following Table 5.1 and the performance are evaluated with the existing the AES and CFES techniques.

**Plain-image Encrypted Image Decrypted Image**

**Lena**



**Pepper**



**Barbara**

**Fig.5.4 Results obtained with Encrypted and Decrypted Image**

From the below Table 5.1 images has been considered for the experimentation and the performance of the proposed approach compared to the approaches such as AES and CFES is shown in Table 5.1. It is observed from the table that the proposed MBECC has better in entropy values for all the standard images taken into consideration. The entropy value 7.03 is obtained for the proposed MBECC respectively which is high when compared to the approaches such as AES and CFES with entropy value of 7.17 is obtained and AES provides the entropy value of 7.99 respectively. The pictorial representation of the experimentation and its performance evaluation are presented in the Fig.5.5 is presented below.

**Table 5.1 Performance Analysis of Entropy Values**

| Images | AES | CFES | Proposed MBECC |
|---|---|---|---|
| Cameraman | 7.99 | 7.14 | 7.03 |
| Baboon | 7.99 | 7.14 | 6.83 |
| Lena | 6.54 | 7.03 | 6.29 |
| Pepper | 6.52 | 6.89 | 5.58 |

The pictorial representation of the experimentation and its performance evaluation are presented in the Fig.5.6 is presented below.

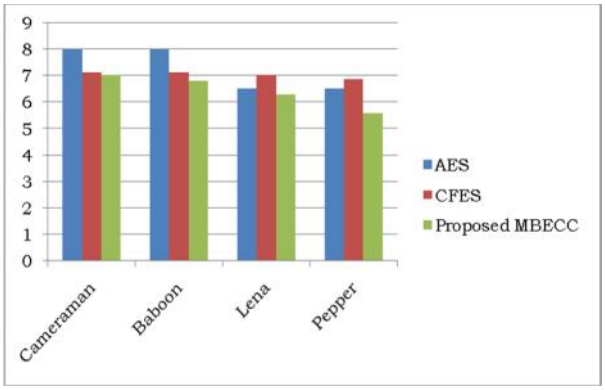



**Fig.5.5 Performance Analysis of Entropy Values**

From the below Table 5.2 shows the experimented values obtained from different methods. The performance was evaluated using the Mean Square Error (MSE). In order to evaluate the performance of the proposed MBECC, the results obtained with the existing techniques such as AES and CFES are compared with the proposed MBECC and are shown in Table 5.2.

**Table 5.2 Performance Analysis of MSE Values**

| Image | AES | CFES | Proposed MBECC |
|---|---|---|---|
| Cameraman | 40.39 | 33.86 | 31.16 |
| Baboon | 40.34 | 33.31 | 32.75 |
| Lena | 39.78 | 33.10 | 32.43 |
| Pepper | 39.75 | 33.06 | 30.17 |

The pictorial representation of the experimentation and its performance evaluation are presented in the Fig.5.6 is presented below.

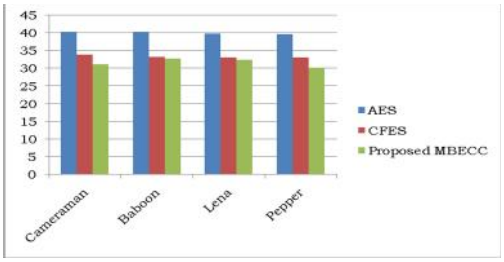



**Fig.5.6 Performance Analysis of MSE Values**

From the above Table 5.3 image blocks has been considered for the experimentation with different sizes. The performance is analyzed with encryption and decryption time is shown in Table 5.3. The speed of encoding and decoding of data is the core advantage of any cryptographic algorithm. The block encryption algorithm is specially designed to reduce the cost and execution time of the process. The following table shows the performance analysis of block encryption algorithm against the some well known algorithms. The following table 5.3 shows the memory required by the image block encryption and decryption. The memory requirement of image block encryption is half as compare to other techniques.

**Table 5.3 Performance Analysis based on Different Block Sizes**

| Image Block Size | Encryption Time (ms) | Decryption Time (ms) |
|---|---|---|
| 8X8 | 20.17 | 22.86 |
| 16X16 | 40.38 | 47.33 |
| 32X32 | 81.57 | 98.16 |
| 64X64 | 165.14 | 203.74 |
| 128X128 | 322.36 | 409.72 |
| 196X196 | 648.49 | 963.63 |
| 256X256 | 611.81 | 922.24 |

The pictorial representation of the experimentation and its performance evaluation are presented in the Fig.5.7 is presented below.

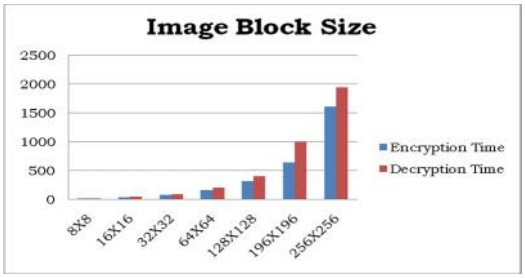



**Fig.5.7 Performance Analysis based on Different Block Sizes**

## 7. Conclusion

In this paper, a matrix base elliptic curve cased crypto technique has been proposed with image blocks for image encryption-decryption has been proposed which utilizes matrix multiplication and inverse matrices. The proposed technique is experimented and compared with existing AES, DES and CFES techniques. Compare with those techniques the proposed model provides better results in image block based encrypt and decrypt efficiently. The performance is evaluated by estimating the MSE and entropy values and compared with methods the proposed MBECC technique provides better encrypting and decryption for images.

## REFERENCES

[1] Akash Kumar Mandal, Chandra Parakash and Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students Conference on Electrical, Electronics and Computer Science, pp.1-5, 2012

[2] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee and SmJmng Kim, Multilevel Image Encryption by Binary Phase XOR Operations, IEEE Proceeding 2003.

[3] Guosheng Gu, Guoqiang Han, An Enhanced Chaos Based Image Encryption Algorithm, IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control in 2006.

[4] Huang-Pei Xiao Guo-Ji Zhang —An Image Encryption Scheme Based on Chaotic Systems, IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, Pp.13-16, 2006.

[5] Obaida Mohammad Awad Al-Hazaimeh, A New Approach For Complex Encrypting and Decrypting Data International Journal of Computer Networks & Communications,Vol.5, No.2, 2013.

[6] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, M., A new modified version of Advance Encryption Standard based algorithm for image encryption, Electronics and Information Engineering, International Conference, 2010.

[7] S.S.Maniccam, N.G.Bourbakis, Lossless image compression and encryption using SCAN, Pattern Recognition,Vol.34, Pp.1229-1245, 2001.

[8] Mohammad Ali Bani Younes and Aman Jantan Image Encryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, vol.35, 2008.

[9] B. Ravi Kumar, P.R.K.Murti Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology, International Journal on Computer Science and Engineering, Vol.3 no.7, 2011.

[10] Santhosh Reddy, owjanya, P. Praveena, Shalini L, Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers International Journal of Scientific and Research Publications, Volume 2, Issue 9, 2012.

[11] Satyajeet R. Shinge, Rahul Patil "An Encryption Algorithm Based on ASCII Value of Data", International Journal of Computer Science and Information Technologies, Vol.5 (6),pp.7232-7234,2014.

[12] Sesha Pallavi Indrakanti,P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications,Vol.28, No.8, 2011.

[13] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, A Modified AES Based Algorithm for Image Encryption World Academy of Science, Engineering and Technology, vol. 27, 2007.