IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Design of efficient compression and cryptographic model for an image transmission using WBCT and ECC

Navyashree R
navyashreer.saru@gmail.com
Bangalore Institute of Technology, Bengaluru, Karnataka

Sujatha S
bit.sujatha@gmail.com
Bangalore Institute of Technology, Bengaluru, Karnataka

ABSTRACT

There is always a need for more memory and enhanced security for transmission. Image compression has gained importance because it reduces the storage space with the only acceptable amount of degrading in quality. Also, cryptographic techniques are used to provide security during transmission. In this project, an efficient compression and cryptographic model for image transmission are proposed. An input image of any format is converted into a grayscale image and Wavelet-Based Contourlet Transform (WBCT) is applied. Wavelets have the capability of approximation of images with sharp discontinuities, but they are not efficient for the approximation of images with a smooth contour. Contourlet transform uses Laplacian pyramidal decomposition and a directional filter bank to produce effective and powerful multiresolution and directional decomposition of an image. Together Wavelets and Contourlet Transform makes an image suitable for image compression. Huffman coding is used for lossless compression of data (image). This compressed image is encrypted using ECC (Elliptic Curve Cryptography). ECC has its own advantages such as smaller keys with enhanced security, requires less computing power, battery life, and memory. The ECC decryption algorithm will perfectly recover the original image. The work is implemented by using MATLAB. The compression ratio is 4.2 to 5 and PSNR value in the range of 24-32.

Keywords— *Contourlet transform, Huffman coding, Wavelet transform, Wavelet Based Contourlet Transform, Elliptic curve cryptography*

1. INTRODUCTION

There is always a need for more memory and it is a never-ending requirement. Many times, we face problems of low storage space whenever we save a file or install a new software. We use mobile phones, computers, pen drives, hard disks, etc. to store images, videos, documents, etc. It is necessary to reduce the size of these elements so that all of them can be stored.

In this project, we aim at compressing the image to the highest compression ratio that is possible. Image compression has gained importance because it reduces the storage space with the only an acceptable amount of degradation in quality. It is a technique used to limit the size of an image in bytes without corrupting the standard of the picture to an unsatisfactory level. This lessening of file size enables more pictures to be put away in a provided memory space. It additionally diminishes the amount of transmission time essential for images when they are sent over the internet.

An image can be compressed in various distinctive manners. The JPEG format and the GIF format are the two most regular compressed graphics image formats in use. The JPEG technique is generally used for photos, whereas the GIF technique is mostly used to draw the line, art and simple geometric shapes in images.

Fractals and wavelets are used for image compression in other compression techniques. These techniques are not very popular on the Internet. In any case, these two techniques offer a guarantee since they offer higher compression ratios than the JPEG or GIF techniques for a few types of images. Another new technique that is capable of replacing GIF format over time is PNG format.

A lossless compression is a compression of program or file where no errors are found up to a certain limit. Errors are included beyond this point. Compression of program or file should be lossless and even a minute error is not acceptable because it causes serious damage to the meaning of file and program code contains error resulting in no run, but in image small degrade in quality is acceptable. In picture pressure, a little misfortune in quality is typically not observable. A "critical point" up to which compression works accurately is not defined, but above that, it is out of possibility. When there is a small acceptance for loss at the point, the value of the compression ratio goes beyond what it can be. Hence, images can be subjected to compression more than text files or programs.

In this project, we consider the input image of any format. At first input image is converted to a grayscale image, later WBCT: Wavelet-Based Contourlet Transform is applied. Thus, this approach provides the advantages of both the Contourlet transform and wavelet. Although wavelets have the capability of approximation of images with sharp discontinuities, they are not efficient for the approximation of images with a smooth contour.

To overcome this Contourlet transform was developed. It uses Laplacian pyramidal decomposition and a directional filter bank to produce effective and powerful multiresolution and directional decomposition of an image. The approximation capacity for smooth 2D signals is good enough. Wavelet-Based Contourlet Transform (WBCT) is a non-redundant version of the above transform which is suitable for image compression.

Cryptography is a technique which deals with mathematical models to enable reliable communication under the influence of intruders. In simple terms, cryptography can be defined as studying, scanning, composing and cracking of code. It disguises the message such that it is difficult to read or unreadable. Thus, it provides a reliable secured way for data transmission across a vulnerable channel. A channel is said to be vulnerable when it is easy for illegal hacking and altering of data.

Cryptography provides confidentiality, data integrity, data authentication, non-repudiation. Encryption is a secured method to disguise the information that is to encode it so that only its lawful user can read it when decrypted. To encrypt data, the encryption algorithm is used to generate ciphertext. Programmers will hack the information data/message, however, won't have the capacity to recover the primitive content as a result of encryption. Symmetric Key Encryption and Public Key encryption are the two types of encryption approaches. In this paper, we use Elliptic-Curve Cryptography (ECC), which is a public-key cryptography approach.

2. LITERATURE SURVEY

Authors P. Vasanthi Kumari and K. Thanushkodi, in [1] defined image compression as a reduction of the size of a graphics file in bytes without reducing its quality to a certain level. In this paper, a new coding technique using the fast Fourier transform and the scalar quantization is presented for standard 'Lena' image and satellite images.

A hybrid encryption algorithm based on Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) algorithms were introduced to provide secured transmission for Meteosat in network communication [2]. Both AES and RSA have its own merits, combining those merits such as efficiency of AES in block encryption and key management of RSA provides improved security to Meteosat.

Applications of wavelets in the area of nonlinear regression and function estimation are discussed in [3].

Kulbir Singh et. al in [4] show the Fourier transforms successful usage in the field of signal processing, image processing, communications, and data compression applications. Particularly for compression of high-resolution satellite images, they showed the generalization of the discrete Fourier transform.

Khaled Sahnoun and co-authors in [5] aim at compressing a large image to ease its storage and transmission with least distortion. In this method first, the image is subjected to fast Fourier Transform (FFT) followed by scalar quantization and then its output is encoded using entropy encoding.

A new method of image compression which is based on wavelets is proposed in [6]. This compression technique uses coding of the wavelet coefficients to give almost lossless compression and is better than classical zero tree.

A brief description of ECC encryption and decryption is given in [7]. Authors groups the pixels and perform elliptic curve operations.

The Advantages of ECC for multimedia encryption is mentioned in [8]. ECC has advantages such as smaller keys, fast computations, battery and bandwidth saving making it suitable for encrypting multimedia.

A new two-pass key exchange protocol based on Diffie-Hellman key exchange protocol to solve the problem of lack of authentication is proposed in [9]. In order to remove the extra cost of transmission and computation caused due to separate authentication, protocols having the capacity of both authentication and key exchange must be used. This proposed protocol works with the Elliptic curves over finite field Fp.

A survey on ECC implementation, mathematical computation, its requirements, advantages, and disadvantages was carried out and results are discussed in [10].

Kristin Lauter in the article, [11] provides an overview of elliptic curves and their uses in cryptography. This paper also sees ECC as a substitute to RSA and in various applications.

3. PROPOSED SYSTEM

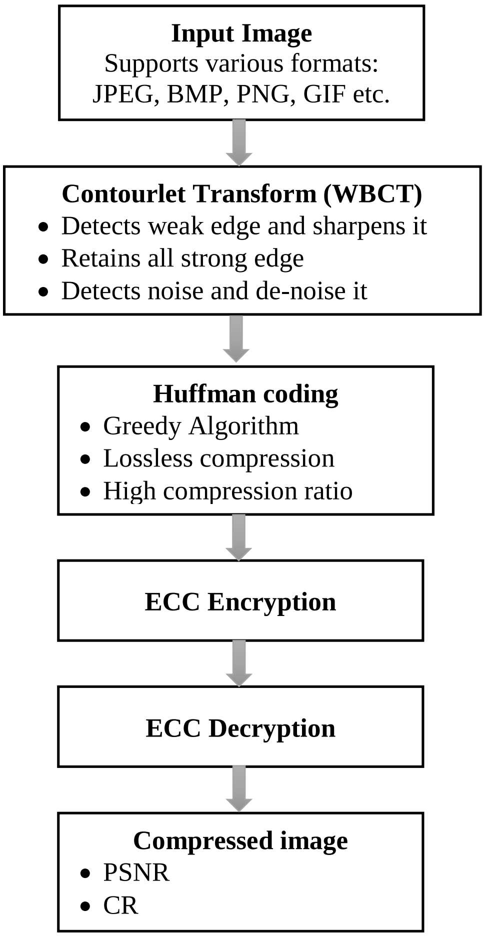

Fig. 1: Block Diagram of Proposed System

The project work is mainly based on the technique of Wavelet-based Contourlet Transform. The pixel value is the only concern in the proposed method. And then quantization is being processed. For compression, Huffman coding is being used for lossless data compression. Finally, the ECC encryption and decryption is being applied to the image only for the authorized person to access the data. Figure 1 shows the block diagram of the proposed method.

The first step is to input the image; the image is read or accepted by the system. The second step is to apply the Contourlet transform. The Contourlet transform was put forth in 2002 by Vetterli and Do. It is an effectively capable multi-resolution, two-dimensional transform having the characteristics of critical sampling, localization, anisotropy and directionality used for the representation of images. Its primary function is to perform multiscale and multi-dimension on an image. This is achieved by wavelet decomposition. Hence the name wavelet-based Contourlet transform.

The third step is Huffman Coding: It is a type of lossless data compression that uses efficient prefix coding. The plan is to assign different-length codes depending on the frequencies of correspondent character to input characters. The more frequently appearing character gets the lowest code value and the less frequently appearing character gets the highest code value.

The fourth step is ECC Encryption: It is the process of manipulating the data or message so that everyone cannot understand it and only authorized people can read the message or access the data after decrypting it. Encryption does not of itself neutralize obstacle but instead restricts the comprehensible substance to a future interceptor. In an encryption plot, the proposed information or message, demonstrated as plaintext is coded with the use of encryption algorithms, delivering cipher message that must be scrutinized if decrypted. For particular reasons, a pseudorandom encryption key is utilized as a part of an encryption strategy produced by an algorithm. It is on a central level possible to disentangle the message without having the key, in the meantime, for a well-developed encryption technique, noteworthy computational resources and capacities are required. An endorsed recipient can without quite a bit of a stretch translates the message with the key given by the originator to recipients yet not to unapproved customers.

The fifth step is ECC Decryption which unlocks the image. The final result is a compressed image without any loss in the image quality. The above block diagram shows the steps used in the proposed system.

3.1. Wavelet-Based Contourlet Transform

In our project, we are using a wavelet-based Contourlet transform. Wavelets are equipped for approximating pictures with sharp discontinuities yet not great at the estimation of pictures with smooth shapes. Consequently, the Contourlet transform was presented. It creates a proficient multiresolution and directional deterioration of a picture utilizing a Laplacian pyramidal decay and a directional channel bank. It has great guess ability for smooth 2D signals. A non-repetitive variant of this transform, Wavelet-Based Contourlet Transform (WBCT) is suitable for image compression.

Wavelets are not ideal in catching the singularities in pictures. The pictures which have surfaces and patterns of oscillatory nature are not successfully spoken to by wavelets. The smooth contours are additionally not effectively spoken to by the wavelet transform.

Contourlet transform is a multi-determination directional transform. It is equipped for catching forms and fire subtle elements in pictures. It is executed as a 2-level disintegration. It has great guess capacity for pictures with smooth contours. Like the wavelet transform, Contourlet transform has a consistent interpretation between the continuous and discrete domain representation. The help for 2D wavelet premise capacities is determined as dyadic squares. The wavelet transform is useful for approximating segregated point discontinuities. Contourlet can proficiently separate the directional highlights with multi-determination ability from pictures with surfaces with smooth shapes. Contourlet transform utilizes a structure like that of curvelets. The plan comprises of double filter bank structure, by consolidating the Laplacian pyramidal decomposition with a directional filter bank. The Contourlet transform beats the ordinary wavelet transforms as far as catching the singularities found in the pictures. In Contourlet transform, a Laplacian pyramidal decomposition of pictures is actualized in the principal arrange. The bandpass yields at different levels of Laplacian pyramids are dissected utilizing Directional Filter Banks (DFB) for separating the angular data. In any case, because of the repetitive nature of Laplacian pyramidal portrayal of pictures, the utilization of Contourlet transform has not turned out to be prevalent for image compression algorithms. So as to have a non-repetitive Contourlet transform, the octave band directional filter banks, the Critically Sampled Contourlet (CRISP) Transform and the wavelet-based Contourlet Transform are proposed.

The proposed WBCT shown in Figure 2 attains both radial and angular decomposition to a random range and meets the anisotropy scaling law of (width= length2). The WBCT is easy to realize by applying DFB on the wavelet coefficients of an image when compared to the DFB-based non-redundant transforms. In this work, to enhance the execution of the Contourlet coder, we utilized the non-redundant WBCT in conjunction with a SPIHT algorithm to build an embedded image coder. Because of contrasts in parent-child connections between the WBCT coefficients and wavelet coefficients, we built up an expounded repositioning algorithm for the WBCT coefficients such that we could have comparative spatial orientation trees (the zero-trees) as the ones utilized for examining the wavelet coefficients.

Its remarkable feature is that it is non-redundant, and it has the capacity for perfect reconstruction. The principal stage gives subband decomposition, which on account of the WBCT is a wavelet change, rather than the Laplacian pyramid utilized as a part of Contourlets. The second phase of the WBCT is a Directional Filter Bank (DFB), which gives angular decomposition. The principal stage is acknowledged by separable filter banks, while the second stage is actualized utilizing non-separable filter banks. For the DFB level, the iterated tree structured filter banks utilizing fan filters are developed. Wavelet coefficients are additionally investigated to break down them with directional filter banks. The information image is parted into different sub-bands utilizing analysis filter banks and wavelet coefficients are estimated. The analysis directional filter banks are utilized to disintegrate all the high-frequency sub-bands into angular sub-bands.

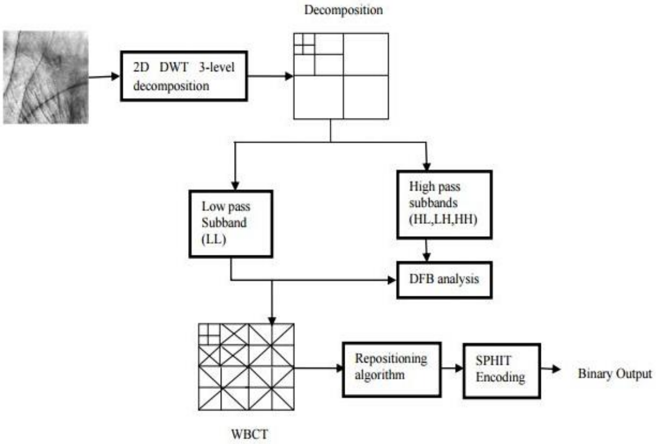

Fig. 2: Flow diagram of the proposed scheme using Wavelet-Based Contourlet Transform

The wavelet decomposition took after by DFB investigation is called Wavelet-Based Contourlet Transform of an image. Like the Contourlet change, the WBCT comprises of two filter bank stages. The primary stage gives sub-band decomposition which, on account of WBCT, is a wavelet transform. The Mallat's Pyramidal disintegration is utilized as a part of the difference to the Laplacian Pyramid utilized as a part of Contourlet. The second phase of the WBCT is the Directional channel bank (DFB) examination which gives angular decomposition. For the DFB organize, the iterated tree structure filter banks utilizing fan filters are utilized. DFB with the rise to a number of directional decomposition to every high pass band at that level of sub-band decay is connected. At n^{th} level decomposition in the wavelet change, the LH, HL and HH detail sub-groups are created. Angular decomposition of wavelet sub-groups is done utilizing DFB with a similar number of bearings to each sub-band at the predetermined level. Course investigation with a most extreme number of bearings is performed on the wavelet sub-groups of the best level. The quantity of headings for the following back to back level sub-band is diminished to fulfill anisotropy scaling law. To segment and refine the huge coefficients in the sub-groups of WBCT, three arrangements of LIP (List of Insignificant Pixels), LIS (List of Insignificant Sets), and LSP (List of Significant Pixels) are produced from the sub-groups as it is determined in the SPIHT coding of wavelet sub-band coefficients. A spatial introduction tree or a zero tree is developed from the wavelet coefficients crosswise over various sub-groups at various scales in view of the parent-kid connection between coefficients. The repositioned coefficients are encoded with SPIHT encoder. Along these lines, a compacted type of info picture is achieved [12].

Figure 3 demonstrates a WBCT encoder. The input data which is an image is part of different sub-groups and wavelet coefficients (Haar) are ascertained for each sub-band. The directional filter banks connected for all the high-frequency components. This blend of wavelet transform and DFB together structures Wavelet-Based Contourlet Transform. Reallocation is done to recognize the location of the children wavelets. The coefficients are encoded with SPIHT encoder. Along these lines, a compressed type of image info is obtained[14].

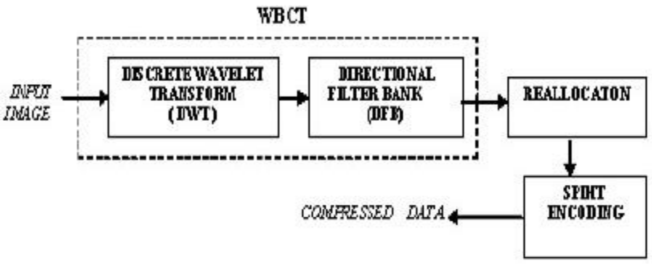
WBCT
INPUT IMAGE
DISCRETE WAVELET TRANSFORM (DWT)
DIRECTIONAL FILTER BANK (DFB)
REALLOCATON
SPIHT ENCODING
COMPRESSED DATA

Fig. 3: WBCT Encoder

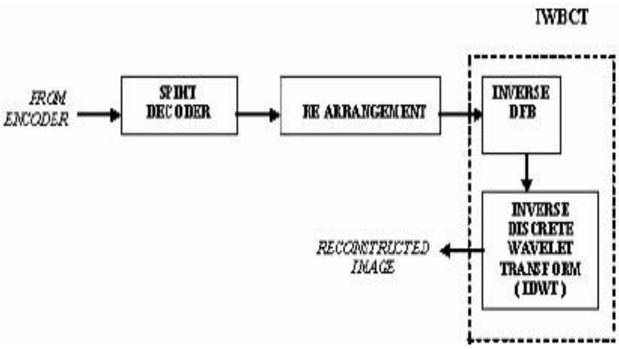

Fig. 4: WBCT Decoder

The encoded picture is given to the SPIHT decoder and every one of the kid wavelets are adjusted. Presently reverse Wavelet-Based Contourlet Transform is connected to the decoded picture. Figure 4 demonstrates a WBCT decoder. In the principal stage inverse, DFB is used followed by backward wavelet change in the following stage. Presently we get a picture around the same as the input data. We find that the picture is preferably recreated utilizing contourlet change over wavelet transform [14].

3.2. Huffman coding technique

In information theory and computer science engineering, a Huffman code is a specific kind of ideal prefix code that is normally utilized for lossless compression of data. The Huffman Coding algorithm was created by David A. Huffman. The last consequence of the Huffman's coding algorithm is a varying-length code table for each of the symbols specified. The algorithm gets this table from the evaluated frequency of occurrence (weight) for every input symbol. Huffman coding encodes every symbol independently and subsequently the least length for every symbol is 1 bit.

The methodology works by making a paired tree of nodes. These are put away in a cluster whose size relies upon the quantity of the source symbols. There are two kinds of nodes, leaf nodes which are the first nodes or the nodes specified in the cluster as said above and the inner nodes made later to substitute these. Leaf nodes contain a connection to a parent node which makes it simple to peruse the code (backward) beginning from a leaf node. Inner nodes contain a weight, connections to two tyke nodes and a discretionary connect to a parent node.

Table 1: Frequency and code table for given symbols.

Symbols	Frequencies	Fixed-Length Code	Variable-Length Code
A	37	000	10
B	18	001	011
C	29	010	111
D	13	011	1101
E	30	100	00
F	17	101	010
G	6	110	1100

As a typical tradition, bit '0' speaks to following the left tyke and bit '1' speaks to following the right tyke. The procedure first considers about the two nodes with least probability and makes another inner node having these two nodes as tykes. The sum of the weight of the tykes gives the weight of the new node. We rehash this procedure until the point that just a single node remains, which is the root of the Huffman tree.

Example: The illustration given below explains Huffman coding [13]. Suppose we want to encode a text with the characters a-g occurring with the following frequencies. Total size is: (37+18+ 29+13+30+17+6)x 3= 450 bits (Fixed-Length Code). Total size is: 37x2 + 18x3 + 29x3 + 13x4 + 30x2 + 17x3 + 6x4 = 402 bits (Variable length Code). A savings of approximately 11%.

3.3. Elliptic Curve Cryptography

There is a number of cryptographic methods available and here we use ECC (Elliptic Curve Cryptography). ECC is a way to deal with public-key cryptography in view of the mathematical structure of elliptic curves over finite fields. ECC needs smaller keys contrasted with non-ECC cryptography (based on the finite field GF(p), where p is a (prime number) to give comparable security [7]. Before ECC end up prevalent, all public key calculations depended on RSA cryptosystem [2], Digital

Signature Algorithm (DSA) and Diffie-Hellman key exchange (DH), elective cryptosystems in view of modular arithmetic. RSA and companions are still vital today and regularly are utilized close by ECC. RSA and companions can be effortlessly clarified, is broadly comprehended, and rough encoding or decoding or digital-signature executions can be composed effectively. Notwithstanding, the establishments and usage abilities of ECC are as yet a riddle and not reasonable to most.

This project gives a straightforward diagram of overview of ECC and makes us familiar about the segmentation of message and orderly map these digital code of segments squares into the points of elliptic curve, after that how to map the image into the elliptic curve points and how to protect it by using the encoding and decoding of ECC. For the arithmetic of the points over an elliptic curve, the algorithm of multiples of points is researched and the investigation is additionally performed. We have explained how the image will map on the elliptic curve cryptography and also have illustrated encryption of plaintext using ECC.

An Elliptic curve is characterized over the integers, real numbers, rational numbers, complex numbers and also finite fields. In this project, we are concentrating just on finite fields. Although for cryptography purpose, elliptic curves can be characterized over various fields that are given above, here we use the elliptic curves that are characterized over a finite field GF(p). An elliptic curve over the finite field GF(p) is the arrangement of points portray by the condition: Ep(a,b): $y^2=x^3+ax+b$ mod p, where $4a^3+27b^2 \neq 0$, p is a prime number. This equation is called Weierstrass normal form for elliptic curves. An ideal point called a point at infinity which is a part of the elliptic curve is characterized for computation of points. This point at infinity is signified by the symbol O(inf,inf).

If we suppose the mod p=23 and the value of a=1 and b=1, E23(1,1) are given in table 2.

Table 2: Points on the Elliptic curve E23(1,1)

(0,1)	(3.10)	(5,19)	(7,12)	(12,4)	(17,3)	(19,5)
(0,22)	(3,13)	(6,4)	(9,7)	(12,19)	(17,20)	(19,18)
(1,7)	(4,0)	(6,19)	(9,16)	(13,7)	(18,3)	----
(1,16)	(5,4)	(7,11)	(11,3)	(13,16)	(18,20)	----

To get the point addition we will choose two points from the elliptic curve points which we generated on table 3 and we will get the point addition on ECC. Let us take the point P=(3,10) and Q=(9,7) after we used the point addition we will get the third point R=(17,20).

To get the point doubling or point multiplication we will choose one point called base point, for example, p=(3,10) and we will apply doubling point by choosing 2p=(7,12), 3p=(19,5), 4p=(17,3).

For encryption one later or more by using elliptic curve cryptography we should choose the base point which we will use in our encryption and decryption technique. We have chosen the (2,4) like a base point(G) on the E5(1,1), so we will start encryption as follows:

1. Alice will choose a private key, for example, na=2 and she will find the public key by using the equation: Pa=na*G , Pa=2*(2,4)=(2,1).
2. Boob will choose the private key, for example, nb=4 and he will find the public key by using the equation: Pb=nb*G, Pb=4*(2,4)=(2.4).
3. Alice and Boob will send their public key to each other.
4. We will find the key exchange to be sure that two (Boob and Alice) share their key correctly, the key exchange is found by using: k1=nb*Pa=4*(2,1)=(2,1), k2=na*Pb=2*(2,4)=(2,1), we can see that k1=k2, that's mean the key exchange has been done correctly.
5. We will map the later (a) on one point on the elliptic curve for example (3,1) and we will suppose that point is the pm(message), so pm=(3,1).
6. Alice will choose the random integer k=2 and she will calculate the ciphertext as following Pc=[kG,pm+kpb] from the Matlab code and she will find the ciphertext as pc=[2,1 0,4] and this value will be sent to the Boob.
7. Boob will decrypt the ciphertext which is sent from Alice by using the same value of the key (K) and reconstruct the original point as following: msg=[pm+kPb-nbkG], he will find the original message as msg=(3, 1) which is representing of (a) later on the elliptic curve.

The encryption and decryption process of image's pixel is the same as the encryption and decryption of one later with mapping the pixel on the image on an elliptic curve.

4. RESULTS AND SIMULATION

In this project, we have selected MATLAB for simulation. MATLAB (Matrix Laboratory) is a mathematical computing environment and fourth-generation programming tool developed by Math Works. MATLAB permits matrix computations, plotting of functions and information, implementation of algorithms, the creation of user interfaces, and interfacing with programs that are written in other languages, including C, C++, Java, and FORTRAN.

In this project, we have shown a secure compressed image transmission using Contourlet transform which includes wavelet decomposition Huffman coding which is a lossless data compression technique and ECC cryptography algorithm to provide confidentiality of data. The execution of the proposed project is done using MATLAB. Below are the results shown for image compression. Figure 5 shows the input image of file size 105 KB. Figure 6 shows the compressed image. Figure 7 represents the encrypted image and figure 8 shows the decrypted image. Here an image file of 105 KB has been compressed to a file size of 23.6KB without a change in resolution. The compression ratio is 4.2 to 5 and PSNR value in the range of 24-32. The results portray a lossless compression technique (Huffman coding). We were able to add ECC encryption technique to this compressed image, which provides security to the image file, allowing only authorized person to access it.

Fig. 5: Input image

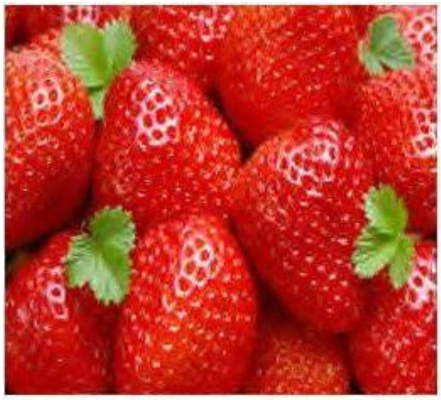

Fig. 6: Compressed image

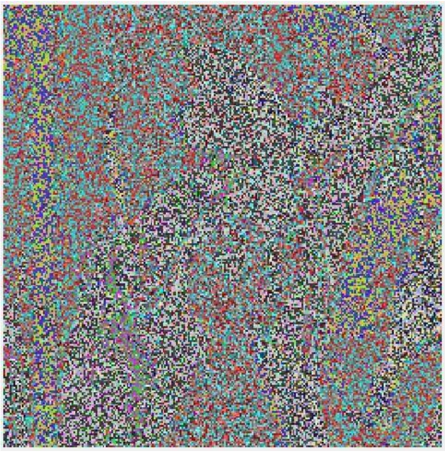

Fig. 7: Encrypted image

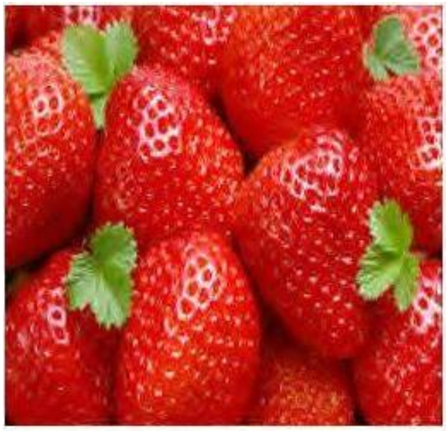

Fig. 8: Decrypted image

Input image:
File size: 105 KB
File format: JPEG
Resolution: 421x342

Compressed image:
File size: 23.6 KB
File format: JPEG
Resolution: 421x342
PSNR: 29

In this project, we have generated the elliptic curve point by using E5(1,1) and from this point, we chose P and Q as a prime number. We applied point addition when p=q (point doubling) or when p q, Also We applied the multiplication scalar for each point to make this point on EC so hard to detect(2p), We generate Diffie-Hellman Key Exchange that will be used in this project. In this project, an image will first transform on EC and then encryption using ECC.

5. CONCLUSION AND FUTURE WORK

We have presented an approach for image compression with a compression ratio of 4.2 to 5 and PSNR value in the range of 24-32. The methods used are Contourlet transform which includes wavelet decomposition Huffman coding which is a lossless data compression technique and ECC cryptography algorithm to provide confidentiality of data. Although methodologies, techniques, and tools used for experimentation were reliable and efficient there always exists a difference between the experimental results. This may be caused as a result of the quality of input data, various minor errors in each stage and few approximations. Since the video is fast moving images, in the future work we will use this method for video storage size compression.

Elliptic curve cryptography is not only used for encryption but also key-agreement protocol and digital signature. ECC useless memory, key pair generation, and signing are considerably faster. This project gives the basic knowledge and convention to understand what elliptic curve cryptography is, moreover, it introduces how to split the image into intensity for ECC and how to map the image into the points of the elliptic curve.

In this project, we have generated the elliptic curve point by using E5(1,1) and from this point, we chose P and Q as a prime number. We applied point addition when p=q (point doubling) or when p q, Also We applied the multiplication scalar for each point to make this point on EC so hard to detect(2p), We generate Diffie-Hellman Key Exchange that will be used in my project. In this project, an image will first transform on EC and then encryption using ECC. The work will be implemented by using MATLAB. The decryption algorithm will perfectly recover the original image. In future, encryption and decryption of a video can also be proposed.

6. REFERENCES

[1] P. Vasanthi Kumari; K. Thanushkodi, “Satellite Image Compression Algorithm Based On the FFT”, 2013 International Conference on Current Trends in Engineering and Technology (ICCTET).

[2] Asma Chaouch; Belgacem Bouallegue; Ouni Bouraoui, “Meteosat Images Encryption based on AES and RSA Algorithms”, 2016 2nd International Conference on ATSIP.

[3] Vikas Gupta; Rajesh Mahle; Raviprakash S Shriwas, “Wavelet-Based Functional Data Analysis: Theory, Applications and Ramifications”, 2013 in Tenth International Conference on WOCN.

[4] Kulbir Singh; Navdeep Singh; Parvinder Kaur; Rajiv Saxena, “Satellite Image Compression using Fractional Fourier Transform”, in 2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[5] Khaled Sahnoun; Noureddine Benabadji, “On-Board Satellite Image Compression Using the Fourier Transform and Huffman Coding”, 2013 World Congress on Computer and Information Technology (WCCIT).

[6] Pengfei Li; XiaoQing Yu; Jingjing Wang, “Wavelet-Based Lossless Compression Scheme with Progressive Transmission Capability”, 2016 International Conference on Audio, Language, and Image Processing (ICALIP).

[7] Laiphrakpam Dolendro Singh; Khumanthem Manglem Singh, “Image Encryption using Elliptic Curve Cryptography”, ScienceDirect, Procedia Computer Science 54 (2015) 472 – 481.

[8] Lo’ai Tawalbeh; Moad Mowafi; Walid Aljoby, "Use of elliptic curve cryptography for multimedia encryption", IET Information Security, 10.1049/iet-ifs.2012.0147.

[9] P. Vasudeva Reddy; M. Padmavathamma, "An authenticated key exchange protocol in elliptic curve cryptography", Taylor & Francis publication, Journal of Discrete Mathematical Sciences and Cryptography, October 2014.

[10] Alessandro Cilardo; Luigi Coppolino; Nicola Mazzocca; Luigi Romano, "Elliptic Curve Cryptography Engineering", Proceedings of the IEEE, vol. 94, No. 2, February 2006.

[11] Kristin Lauter, "The Advantages of Elliptic Curve Cryptography for Wireless Security", IEEE Wireless Communications, February 2004.

[12] V. Mohan, Y.Venkataramani, "Palmprint Compression using Wavelet-based Contourlet Transform and SPIHT", International Journal of Computer Applications (0975 – 8887), Volume 91 – No.10, April 2014.

[13] Mukta Sharma; R. B. Garg "DES: The oldest symmetric block key encryption algorithm"2016 International Conference System Modeling & Advancement in Research Trends (SMART)Year: 2016.

[14] Ramin Eslami; Hayder Radha, "Wavelet-Based Contourlet Transform and its Application to Image Coding", IEEE International Conference on Image Processing (ICIP 2004), Vol. 5, pp. 3189-3192, Oct. 2004.